Privacy Organisational Model

Approved by the Board of Directors of ERG S.p.A. on 15th October 2024

Contents

1. DEFINITIONS

In addition to the definitions contained in other parts of this "Privacy Organisational Model" (hereinafter referred to as the "Organisational Model" or the "Model"), the terms and expressions with capitalised initials used hereinafter have the meanings assigned to them below, it being understood that the same meaning applies both in the singular and in the plural:

- **System Administrator**: natural person who is responsible, in the name and/or on behalf of Group Companies, for the management and/or maintenance of an IT and data processing system or its hardware and software components.
- **Supervisory Authority**: public authority in charge of supervising the application of the legislation on the protection of Personal Data and in particular of the GDPR in order to protect the fundamental rights and freedoms of natural persons with regard to the Processing (for example, for Italy, it must be understood the Italian Data Protection Authority).
- **Authorised Person**: natural person authorised to materially carry out the Processing operations on behalf of the Data Controller. With reference to the Group Companies, all staff are authorised, by virtue of the duties performed on the basis of the Organisational Manual, to perform the processing of Personal Data, as well as members of the management bodies (other than the Privacy Representative) and monitoring bodies of all the Group Companies, including the members of the related Supervisory Bodies, limited to their respective areas of competence.
- **CISO or Chief Information Security Officer**: Staff responsible for the IT security strategy and its implementation to ensure the security and protection of the ERG Group's systems.
- **DPIA or Data Protection Impact Assessment**: an activity aimed at assessing the consequences that the Processing might have on the rights and freedoms of Data Subjects, as a result of which Security Measures proportional to the risk of the Processing are defined in order to mitigate it to an appropriate extent.
- **Common Data**: any Personal Data other than Judicial Data and Special Data.
- **Judicial Data**: any Personal Data relating to criminal convictions, offences or related security measures.
- **Special Data**: any Personal Data suitable for revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as relating to genetic data, biometric data, data relating to health or sexual life or the sexual orientation of the person.
- **Data or Personal Data**: any information relating to an identified or identifiable natural person; a natural person is considered identifiable who can be identified, directly or indirectly, with particular reference to (i) an identifier such as the name, an identification number, location data, (ii) an online identifier or (iii) one or several characteristic elements of its physical, physiological, genetic, psychological, economic, cultural or social identity of which a Group Company is the Owner, Data Processor or Sub-Processor.
- **Privacy Representative**: the natural person to whom the Data Controller has conferred all the powers and responsibilities on decisions regarding the purposes and methods of the Data Processing, including the security profile.
- **Privacy Provisions or Provisions**: pro tempore laws and regulations in force in all countries in which the Companies of the Group provide (in whole or in part) their activities, concerning the protection of Personal Data.
- **ERG**: ERG S.p.A.
- **ERG Power Generation**: ERG Power Generation S.p.A.
- **GDPR**: Regulation (EU) 2016/679 on the protection of Personal Data.
- **ERG Group or ERG Group Company: ERG and its Subsidiary Companies**
- **Subject or Data Subject**: the identified or identifiable natural person to whom the Personal Data refers (including employees, candidates for recruitment, suppliers, business partners, members of the management and control bodies of the Group Companies, participants in events, visitors).
- **ISMS Committee**: responsible for coordinating the various organisational units of the Group

involved in the management of IT security incidents, also relating to Personal Data.

- **Organisation Manual:** a document which, given the ERG Group's framework at any given time and for each position found within the company's Organisation Chart, defines:
  - the purpose, understood as being the main objective.
  - the responsibilities, with regard to the macro-activities of the main processes.
  - the expected range of their technical (expertise) and managerial competence.
- **Security Measures**: technical and organisational measures aimed at guaranteeing the protection of Personal Data.
- **Internal regulations**: all the regulations adopted by the ERG Group.
- **Staff, or Staff of the ERG Group**: all persons who have an employment contract with one of the ERG Group Companies (including staff on internships, apprenticeships and temporary contracts).
- **Privacy by Default**: principle on the basis of which in each Processing the appropriate Security Measures must be adopted by default to ensure that only the Personal Data necessary for each specific Processing purpose are processed.
- **Privacy by Design**: principle on the basis of which the definition of Security Measures must take place right from the design of each business process, with particular reference to the related supporting IT applications.
- **Privacy Focal Point:** Staff identified by the Data Processor, with the support of ERG's Organisation organisational unit, having consulted the head of the organisational unit concerned by the aforementioned appointment, in order to facilitate - with reference to one or more Group Companies - the management of some of the issues and obligations pertaining to the Data Processing within the relative organisational unit to which it belongs and supporting the Privacy Officer of the Data Processing.
- **Profiling**: any form of automated Processing consisting in the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or travel of that natural person.
- **Privacy Officer**: Staff identified by the Privacy Representative and belonging to the Compliance 231 & Privacy organisational unit with the task of managing - with reference to one or more Group Companies - some of the issues and obligations relating to the Processing of Personal Data and supporting the Privacy Representative.
- **Record or Record of Processing activities**: record of Processing activities performed by the Data Controller or by Data Processors on behalf of the Data Controller.
- **Data Processor**: the natural or legal person (including Group Companies), public authority, agency or other body that processes Personal Data on behalf of the Data Controller (e.g. suppliers).
- **Subsidiaries**: subsidiaries controlled by ERG pursuant to Art. 93 of the Consolidated Financial Law.
- **Sub-Processor**: the natural or legal person (including Group Companies), public authority, agency or other body that processes Personal Data on behalf of the Data Processor.
- **Third Parties**: legal entities (including Group Companies) or natural persons (other than those Authorised to Process) to whom the Group Companies, as Data Controllers, may make certain Personal Data available and who, in some cases, operate as Data Processors.
- **Data Controller**: the natural or legal person (including the Group Companies), public authority, agency or other body which, individually or together with others, determines the purposes and methods of the Data Processing as well as the instruments used.
- **Processing:** any operation or set of operations, performed with or without the aid of automated processes, and applied to Personal Data or sets of Personal Data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, communication by transmission, dissemination or any other form of provision, comparison or interconnection, restriction, deletion or destruction.
- **Personal Data Breach or Data Breach**: any event that accidentally involves, or offence that involves, the destruction, loss, modification, unauthorised disclosure or access to Personal

Data transmitted, stored or otherwise processed by the Data Controller.

2. PURPOSE AND SCOPE OF APPLICATION

Through the Model, the Internal Regulations are identified and the Security Measures adopted to guarantee compliance with the Privacy Provisions in force in all the countries in which the ERG Group Companies carry out (in whole or in part) their activities are defined.
Implementation of the Organisational Model is mandatory for ERG and for all Group Companies. The Model was approved by the Board of Directors of ERG and, progressively, by competent corporate bodies of each Company of the Group.

All ERG Group Staff are responsible for the application of the Model, with particular reference to those Authorised to Process, who must actively contribute to the protection of the Personal Data subject to the Processing as well as compliance with the Privacy Provisions.
Compliance with the provisions of the Model must be considered an essential part of the contractual obligations of the Staff of the ERG Group.
Third Parties that have relationships with Group Companies must be aware of the Model and comply with it in all aspects that pertain to their activities carried out in the interest or on behalf of the Group Companies.

3. REFERENCES

External references

- Regulation (EU) 2016/679;
- Personal Data Protection Code, Legislative Decree No. 196 (also, hereinafter, the “Privacy Code”), as amended by Legislative Decree No. 101 of 2018;
- Measures issued by the Italian Data Protection Authority, including in particular: Provision of the Italian Data Protection Authority - 27 November 2008 - Measures and precautions prescribed to the data controllers carried out with electronic instruments in relation to the attributions of the functions of system administrator;
- UK Data Protection Act 2018;
- Regulations and provisions on the protection of Personal Data issued by the Supervisory Authorities of the countries in which the ERG Group operates (e.g. Spain, France, Germany, UK) on the protection of Personal Data;
- ISO/IEC 27001/2022: Information security, cybersecurity and privacy protection - Information security management system.

Internal references

- Code of Ethics;
- “Data breach management” Procedure;
- "Management of Inspections" Procedure.
- "Crisis Communication Management" Guidelines;
- "Whistleblowing" Guidelines;
- PR-ISMS-11.1_"IT incident management" Procedure;
- PR-ISMS_11.0.3_ "Corporate Information Security Regulation" Procedure;
- POL-ISMS_ 4.0.1_"Information Security" Policy;
- PR- ISMS-11.0.6_ "Information Classification" Procedure;
- PR-ISMS-7.2_"IT incident management" Procedure;
- Organisational and management models pursuant to Legislative Decree No. 231/01, adopted by the Italian companies of the ERG Group, where applicable.

4. PRIVACY PRINCIPLES

In carrying out all Processing activities, the ERG Group operates in compliance with the following

principles:

- lawfulness, fairness and transparency of the Processing with respect to the Data Subject;
- limitation of the purpose of the Processing, including the obligation to ensure that any subsequent Processing is not incompatible with the purposes of the collection of Personal Data;
- minimisation of the Data, in the sense that the Personal Data must be adequate, relevant and limited to what is necessary with respect to the purposes of the Processing;
- accuracy and updating of the Data, including the timely cancellation or adjustment of Personal Data that are inaccurate with respect to the purposes of the Processing;
- limitation of storage, or the need to provide for the storage of Personal Data for a time not exceeding that necessary with respect to the purposes for which the Processing was carried out;
- integrity and confidentiality, ensuring that the security of the Personal Data subject to the Processing is adequate;
- accountability, understood as the commitment to implement adequate Security Measures to ensure that the Processing is performed in compliance with the Regulatory Provisions, providing adequate demonstration of the fulfilment of this commitment.

5. ORGANISATIONAL MODEL: ROLES AND RESPONSIBILITIES

The ERG Group has defined an internal organisational structure (hereinafter the "Privacy Organisation") dedicated to the protection of Personal Data, consisting of the following figures:

- Data Controllers;
- Privacy Representatives;
- Data Processors and Sub Processors;
- Privacy Officers;
- Authorised Persons;
- Privacy Focal Point;
- Head of Compliance 231 & Privacy;
- Chief Information Security Officer (CISO);
- Head of ICT Governance, Integration & Security;
- System Administrators;
- Chief Audit Officer.

If the Privacy Provisions require the appointment of a Data Protection Officer (hereinafter the "DPO"), the related Privacy Representative shall appoint one. The DPO will be required to perform the activities expressly mentioned in the aforementioned Provisions while taking into account the Privacy Organisation.
Annex 1 to this document shows the chart with the Privacy Organisation.

5.1. Data Controllers and Privacy Representative

Each Data Controller is responsible for determining the purposes and methods of the Processing, as well as the tools used, and specifically has the task of defining:

- The type of Personal Data to be processed;
- The methods and systems used for the Processing;
- Purpose of the Processing;
- The need to transfer Personal Data to Third Parties;
- The methods and storage period of the Personal Data;
- Security Measures to be adopted for the protection of Personal Data.

In consideration of the above, each Group Company acts as Data Controller in relation to the Processing performed in its own interest (i) directly and/or (ii) by Third Parties (including Group Companies) on its behalf.

Each Data Controller designates a Privacy Representative, or natural person to whom the Data

Controller confers all the powers and responsibilities in respect of the decisions made in relation to the purposes and methods of each Processing.

The Privacy Representative (i) in the case of a collective management body, is appointed through a specific decision of the management body or (ii) in the case of a single management body, coincides with the sole director.

5.2. Data Processor and Data Sub-Processor

Each Group Company, as Data Controller, appoints as Data Processors all the Third Parties (including Group Companies, suppliers or business partners) who carry out the Processing on its behalf and in the interest of the same.
The Data Controller, depending on the case, may authorise the Data Processor to appoint one or more Third Parties (including Group Companies) as Data Sub-Processor(s). The Data Sub-Processor accordingly designated is required to comply with the same obligations established in the contract entered into between the Data Controller and the Data Processor, who remains fully responsible for compliance with the obligations relating to the Processing by the Sub-Processor.
The Data Controller must only make use of Data Processors who ensure sufficient guarantees to put in place adequate Security Measures so that the Processing is in line with the Privacy Provisions and guarantees the protection of the rights of the Data Subject.

The appointment of the Data Processor and the methods of Processing by the same are governed by a contract through which the following are defined, in particular:

- The object and duration of the Processing;
- Purpose of the Processing;
- The type of Personal Data processed, and the categories of Data Subjects involved;
- Instructions/restrictions for any transfer of Personal Data;
- The application of adequate Security Measures;
- The obligations and rights of the Data Controller and the Data Processor.

In particular, the Data Processor is responsible for:

- ensuring that the Processing takes place according to the instructions given by the Data Controller;
- adopting all appropriate technical and organisational measures to guarantee the security of the Processing;
- requesting the written authorisation of the Data Controller in order to appoint and be able to rely on a Sub-Data Processor;
- proceeding with identifying, within its own structure, the persons who are authorised to perform Processing, providing them with appropriate instructions regarding the Processing performed/to be performed, and ensuring that they are bound by legal confidentiality obligations;
- monitoring the Processing operations performed by its Authorised Authorities and ensuring that they are carried out in compliance with the instructions given to them and only in relation to the areas of Processing allowed to them;
- promptly inform the Data Controller of the requests of the Data Subjects that may reach the Data Processor and collaborate with the Data Controller in order to guarantee the effective exercise by the same of all the rights provided for by the Privacy Provisions;
- promptly informing the Data Controller of any breach, including a potential breach, of the processed Personal Data;
- allowing the Data Controller to conduct inspection tasks relating to the methods of execution for the Processing.

In case of doubts regarding the possible qualification of a Third Party as a Processor, the Compliance 231 & Privacy organisational unit should be contacted to obtain guidance on the subject.

The Group's organisational model provides the centralisation of shared activities within the ERG

Group Companies. In particular, ERG guarantees strategic direction and is directly responsible for the business development and management of all business support processes for all Group companies through an intercompany contract with ERG Power Generation which, in turn, has similar intercompany contracts with other Group companies (hereinafter the “Intragroup Contracts”).

Under the scope of Intragroup Contracts,

- ERG, in relation to the Processing performed in the interest and on behalf of ERG Power Generation, acts as Data Processor;
- ERG Power Generation, in relation to the Processing preformed in the interest and on behalf of other Group Companies, acts as Data Processor;
- ERG, in relation to the Processing carried out in the interest of other Group Companies, but on behalf of ERG Power Generation, acts as Sub-Processor.

5.3. Privacy Officer

Each Privacy Representative of Group Companies with Staff may, depending on the case, designate a Privacy Officer. The latter may be identified from Staff within the Compliance 231 & Privacy organisational unit, who due to their experience, ability and reliability, are able to support the Privacy Representative in compliance with the Provisions, including the security profile.
In undertaking his/her assignment, the Privacy Officer must comply with the instructions received from the Privacy Representative.

In particular, the Privacy Officer has the task of:

- providing the Privacy Representative all the information necessary to demonstrate compliance with the obligations relating to the Provisions;
- providing advice to the Privacy Representative and the Authorised Parties on issues relating to the Processing;
- providing, if requested, opinions on the keeping of the Record of Processing Actvities and the performance of the DPIA;
- promptly informing the Privacy Representative of any breaches in relation to the Processing.
- signing and formalising the appointments as Data Processor;
- signing and formalising, with the support of the organisational unit of ERG Organisation, the appointments to Privacy Focal Point, having consulted with the head of the Organisation unit affected by the aforementioned appointment;
- signing and formalising the appointments as System Administrator, on the recommendation of the Information & Communication Technology organisational unit;
- supporting the Privacy Representative in any interaction with the Supervisory Authority, or any other Public Authority, in case of a request for information or providing checks on and access to the Personal Data processed by the Data Controller;
- providing periodic training to the Staff of the ERG Group on the Processing of Personal Data;
- keeping up to date on the changes made to the Privacy Provisions and evaluate the related adjustment methods.

5.4. Authorised Persons to Process Data

Staff who, by virtue of the duties performed on the basis of the Organisation Manual, are set the task of processing Personal Data, as well as members of the management bodies (other than the Privacy Representative) and control bodies of all the Group Companies, including the members of the related Supervisory Bodies, are authorised to process data.
Each Authorised Person must limit himself/herself to processing Personal Data in accordance with the scope strictly necessary for the performance of his/her duties or assignments and has in particular the task of:

- processing Personal Data lawfully and fairly;
- checking that the Data is relevant, complete and not exceeding the purposes for which it was collected and subsequently processed;

- promptly informing the Privacy Officer if there is a need to provide Processing operations for purposes or using methods other than those resulting from the instructions received;
- ensuring that Personal Data is accurate and up to date, from collection to destruction, while preventing access to unauthorised third parties;
- ensuring the traceability and re-traceability of Personal Data (access, changes and archiving) throughout its life cycle;
- keeping the Data only for the duration necessary for the purpose indicated and/or for the time required in compliance with the Security Measures prepared by the CISO, after consulting the Privacy Representative;
- communicating or transferring Personal Data exclusively to other Authorised Parties and/or Third Parties entitled to receive it, for the purposes for which the Data was collected and in any case in compliance with the instructions received;
- promptly informing the Compliance 231 & Privacy organisational unit of the requests of the data subjects that may be received and collaborating with it in order to guarantee the effective exercise by the Data Subjects of all the rights required by the Provisions.

In case **of a Data breach** (i.e. intentional or unintentional destruction, loss, modification, disclosure or unauthorised access to the Data transmitted, stored or otherwise processed), the Authorised Person will be required to promptly communicate this breach to the Privacy Officer, the Head of Compliance 231 & Privacy and the Head of ICT Governance, Integration & Security, who will call the ISMS Committee to a meeting. The Privacy Representative must subsequently notify the Supervisory Authority, without undue delay and where possible, **within 72 hours** of the moment when the Personal Data breach event was detected.
In case of doubts or issues relating to the application of the Model, each Authorised Party must contact the Compliance 231 & Privacy organisational unit to obtain information on the matter.

5.5. Privacy Focal Point.

Each Privacy Officer of Group Companies with Staff, with the support the organisational unit of ERG Organisation, after consulting the head of the organisational unit concerned, may designate one or more Privacy Focal Points, to be identified from the Staff within the organisational units of the Group, who due to their experience, ability and reliability are able to provide support to the Compliance 231 & Privacy organisational unit and/or to the Privacy Officer assigned to carry out the correct Data Processing.
The Privacy Focal Point, in relation to the organisational unit to which it belongs, has, in particular, the task of:

- collaborating with the Privacy Officer and the Compliance 231 & Privacy organisational unit in the execution of the obligations required by the Privacy Provisions;
- involving the Privacy Officer and/or the Compliance 231 & Privacy organisational unit in case of any new Processes to be carried out or changes to existing Processes;
- providing the 231 Compliance & Privacy organisational unit with the information necessary for updating the Record of Processing Activities and, where necessary, for carrying out the DPIA.
- collaborating with and contributing to control activities (e.g. internal audit or inspections of the Control Authority) by providing all the requested information;
- participating in training and refresher sessions (e.g. training on specific topics, working groups);
- reporting any critical issue relating to the Processing.

In case of doubts or questions relating to the application of the Model, each Privacy Focal Point must contact the Compliance 231 & Privacy organisational unit to obtain information on the matter.

5.6. Compliance 231 & Privacy

The Compliance 231 & Privacy organisational unit has the following main tasks:

- operationally supporting the Privacy Officers in the performance of their duties;

- proposing the adoption and/or updating of relevant Data protection procedures;
- coordinating the activities for updating the Record of Processing Activities and for carrying out the DPIA;
- preparing the Privacy Notice and Consent to Processing;
- managing responses to requests from Data Subjects;
- supporting the organisational units and, in particular, the Privacy Focal Points in case of doubts on questions relating to data protection and in the development of new projects;
- cooperating in the management of Data Breaches;
- cooperating with the CISO and with the ICT Governance, Integration & Security organisational unit, with regard to the issues under its responsibility (i.e. IT security and definition of Security Measures);
- improving the efficiency of data protection processes.

5.7. Chief Information Security Officer (CISO).

The CISO is responsible for the management of technical and IT security aspects in the field of Data Processing and operates through the ICT Governance, Integration & Security organisational unit.

In particular, the CISO has the task of:

- managing the ERG Group's IT security strategy and its implementation to ensure that the company's systems, services and information, including Personal Data, are adequately secure and protected.
- defining, maintaining and communicating the vision, strategy, policies and procedures of IT security.
- managing the implementation of the IT security policy throughout the Group.

5.8. ICT Governance, Integration & Security

The ICT Governance, Integration & Security organisational unit ensures the development and regular alignment of ICT Governance & Security with the needs of the ERG Group, guaranteeing adequate methods and tools for integration and data management and implementing the IT security strategy so that the systems, services and Personal Data are adequately safe and protected, in line with the principles of "Privacy by Design" and "Privacy by Default".

The ICT Governance, Integration & Security organisational unit specifically has the task of:

- identifying suitable and preventive Security Measures aimed at guaranteeing a level of security adequate to the risk of the Processing, in order to ensure the confidentiality, integrity, availability of the Processing systems and activities;
- periodically updating the Privacy Officer and the Compliance 231 & Privacy organisational unit with regard to new projects that involve the adoption of systems for the Processing of Personal Data and, in general, the status of implementation of the Security Measures required to protect Personal Data in compliance with the defined criteria;
- providing technical support for any organisational unit that processes Personal Data, through the use of company information systems;
- identifying the internal System Administrators, ensuring adequate supervision of the operational activity carried out (collection and monitoring of logs, periodic verification activities on the activity carried out, storage of the identification details of the system administrators);
- verifying that the disposal of electrical and electronic waste containing Personal Data takes place in accordance with the provisions of the applicable legislation, or if this activity is entrusted to an external supplier, ensuring that adequate Security Measures are adopted;
- technically defining logical Security Measures for access to electronic databases and adequate physical Security Measures for access to data centre rooms;

- convening the ISMS Committee responsible for coordinating the various organisational units involved in the management of IT security incidents also relating to Personal Data, in compliance with the Privacy Provisions and Internal Regulations;
- implementing specific notice flows, in compliance with the "Data Breach Management" Procedure, in case of breaches of the Personal Data detected or in case of anomalies that may lead to the presumption of possible compromise of such data, collaborating with the Privacy Officer for the prescribed obligations relating to notice to the Supervisory Authority and the Data Subject where necessary;
- promptly communicating the restoration of availability and access to Personal Data in the event of a physical or technical incident.

5.9. Internal Audit

As part of the Audit Plan, the Internal Audit organisational unit may perform checks in relation to compliance of the ERG Group with the rules defined in this document, also with the support of other organisational units such as Compliance 231 & Privacy and Information & Communication Technology.
Internal Audit informs the Privacy Officer and the Data Controller about the results of the audit conducted as part of the Processing of Personal Data.

6. COMPANY MANAGEMENT MODEL

Processing operations must be strictly limited to the tasks necessary to pursue the purposes indicated in the Privacy Notice and, in any case, must be compatible with said purposes.
The phases of the life cycle of the Personal Data are shown below, which contain the operation methods:

- Collection.
- Processing.
- Termination of Processing and Cancellation.

6.1. Collection

6.1.1 Purpose

The Processing of Personal Data by the Companies of the ERG Group must take place for the pursuit of legitimate purposes identified in advance.
The Personal Data (collected or received) must be adequate, relevant and limited to the tasks necessary for the purposes of its processing.
Some purposes are reported below, merely by way of example:

- selection and recruitment of Staff and management of the employment relationship with them;
- management of relations with customers, suppliers and business partners;
- management of relations with the members of the management and control bodies of the Group Companies;
- management of access to the offices of the Group Companies;
- protection of the safety of people or property by using video surveillance tools;
- analysis of preferences/choices and statistical processing;
- management of user registrations on the websites/platforms of the ERG Group;
- Profiling activities.

6.1.2 Legal basis

Each Processing requires the identification of the legal basis that legitimises it.
Regarding to the Personal Data processed within the ERG Group, the legal bases of the Processing are:

a. **consent**: when the Processing is explicitly authorised by the Data Subject for one or more specific purposes (e.g. Processing of Particular Data or Judicial Data) (the "Consent to Processing").
   In order for the processing based on this legal basis to be considered lawful, the Consent to the Processing must be expressed through a positive act in which the Data Subject expresses his/her free, specific, informed and unequivocal intention to accept the Processing of Personal Data that concerns him/her, or a written declaration (also by electronic means, e.g. by selecting a specific box on a website).
   Data Subjects have the possibility to revoke the Consent to the Processing previously given to the performance of certain processing operations at any time. In these cases, the Processing operations performed in accordance with this consent must be promptly interrupted unless there is another legal basis for the Processing.

b. **The execution of a contract or pre-contractual provisions**: when the Processing is connected to the execution of a contract of which the Data Subject is a party or to the execution of pre-contractual measures adopted at the request of the same (for example, to hire a candidate it will be necessary to collect his/her personal data such as name, last name, address, etc.).
   In order for the Processing based on this legal basis to be considered lawful, the following is required:
   - there must be a valid contract between the Group Company and the Data Subject;
   - the Processing of the Data provided by the Data Subject is objectively necessary for the execution of the contract;
   - the Privacy Notice is provided to the Data Subject with an indication of the legal basis of the Processing.

c. **the fulfilment of a legal obligation:** when the Processing is imposed by a law, and/or regulation (e.g. administrative and tax obligations: payslip management).
   In order for the Processing based on this legal basis to be considered lawful, the following is required:
   - the obligation must be defined by the European or national law of a State;
   - these provisions must establish an imperative obligation of sufficiently clear and precise Processing;
   - these provisions must at least define the purposes of the processing in question;
   - this obligation must be imposed on the Data Controller and not on the Data Subjects.

d. **The legitimate interest of the Data Controller:** when the Processing is necessary for the specific needs of the Data Controller, provided that the Processing is not excessively invasive for the Data Subject (e.g. installing a video surveillance system for security purposes).
   In order for the processing based on this legal basis to be considered lawful, a balance must be carried out between the interests of the Data Controller and the recognised rights of the Data Subject in order to assess and demonstrate the prevalence of the interests of the Data Controller over the rights of the Data Subject.
   In balancing interests, it is necessary to evaluate:
   - whether the Processing is really necessary taking into account the possible harm that would result to the Data Controller if he/she did not carry out the Processing;
   - the impact on the Data Subjects and their reasonable expectation of what will happen to their Personal Data;
   - the presence of additional Data protection measures that may limit the impacts of the Processing on the Data Subjects.

6.1.3 Privacy Notice

The Data Controller must provide the Data Subject with all information relating to the Processing of Personal Data concerning him/her, in a concise, understandable and easily accessible form, in

simple and clear language, in writing or by other means, including in electronic format (website) (the "Privacy Notice").
The Privacy Notice is structured by indicating at least the following elements:

- the identification details of the Data Controller and the relative methods of contact;
- Purpose of the Processing;
- the legal basis on which the Processing is based;
- the categories of Personal Data;
- whether or not the contribution of Personal Data is mandatory and the consequences of any rejection;
- the possibility of transfer to countries located outside the European Union, if applicable.
- the recipients or any categories of recipients of the Personal Data;
- the storage period or, where it is not possible to define it in advance, the criteria used to determine it.;
- contact details in order to exercise their rights;
- the existence of the recognised rights of the Data Subject;
- the right to lodge a complaint with the Supervisory Authority;
- the existence of any automated decision-making process (without human intervention), including profiling, the logic applied and the consequences for the Data Subject;
- the source from which the Data is acquired if it is not provided to the Data Controller directly by the Data Subject.

The Privacy Notice must be provided to the Data Subject at the time of collection of the Personal Data or, if the Data are obtained from another source, within a reasonable time but within one month at the latest.

In case new Processes or new methods of carrying out pre-existing Processes take over, it will be the responsibility of each organisational unit to contact the Data Processor in advance, including through the Privacy Focal Point, in order for all the in-depth analyses and activities to be implemented (analysis of the Privacy Provisions), risk and security analysis, integration of the Privacy Notice).

6.2. Processing - General principles

The processing operations performed by the Companies of the ERG Group must comply with the principles and general rules dictated by the regulations and referred to in Art. 4 of the Model.

6.3. Termination of Processing - Cancellation and Destruction

In order to ensure that Personal Data are not stored longer than necessary, a deadline must be established for the termination of the Processing and for the cancellation or anonymisation.
The Group Companies must:

- define a storage period of the Personal Data in relation to the specific purposes of the Processing;
- ensure that the storage period of the Personal Data is limited to the minimum time necessary;
- take all reasonable steps to delete or anonymise the Data, without prejudice to the defined storage period and without prejudice to the obligations related to legal obligations or defensive purposes.

7. OPERATING RULES: MACRO PROCESSES

7.1. Record of Processing Activities

Each ERG Group Company with Staff, which processes Data as Data Controller or as Data Processor, where required by the provisions of the GDPR, is required to fill in the Record with reference to the processing activities performed under its responsibility.
The Record of Processing Actvities must include, inter alia, the following information:

- Data Controller and Privacy Representative;

- organisational unit: organisational structure of the Group Company that uses Personal Data to carry out its work activities;
- Purpose of the Processing: purpose of the Data collection;
- categories of Personal Data processed: Common Data, Particular Data and Judicial Data;
- role assumed in the Processing: indicates whether the Processing is carried out as Data Controller, Data Processor or Sub-Processor;
- category of the Data Subject: macro-classification of the Data Subject (e.g. employees, candidates for recruitment, suppliers and business partners if natural persons, members of the management and control bodies of the Group Companies, participants in events, visitors).
- storage period: data storage period, also communicated to the Data Subject by means of the Privacy Notice;
- general description of the Security Measures adopted;
- DPIA: possible execution of a data protection impact assessment for the Processing of Personal Data;
- IT systems used and archives (physical and logical);
- categories of Third Party recipients (name of the legal entity that processes/receives the Data);
- possible transfer of the Data outside the EU.

The Record of Processing activities is one of the main elements of accountability of the Data Controller and constitutes an integral part of the system for the correct management of Personal Data and the Model.
The Record is drawn up in writing and in electronic format and must be kept available to the Supervisory Authority.

7.2. Privacy by design and by default

Data protection, according to the principles of Privacy by Design and Privacy by Default, must:

- be integrated within the life cycle of the processes/systems/applications in which Personal Data is processed from the time of design;
- consider the entire life cycle of Personal Data, from collection to deletion, also taking into account the transfer, storage, processing, consultation and communication;
- safeguard the confidentiality, integrity and availability of the Personal Data processed;
- provide that by default of the processes/systems only the Personal Data necessary for each specific purpose of the Processing is processed;
- provide that by default of the processes/systems, the processed Personal Data is not made accessible to an indefinite number of natural persons, without a real need and the consent of the Data Subject (where applicable).

The principles of Privacy by Design and Privacy by Default must be integrated into the entire organisation of the ERG Group. Therefore, all organisational units must pay attention to ensuring that the development of projects, organisational processes, IT systems, products and services is subject to a prior audit, in order to assess the impact for the purposes of the processing of personal data from the design stage while identifying any appropriate measures to contain the risk and update the Record of Processing Actvities.
This requires that there is extreme awareness of the importance of data protection within the Group and that each organisational unit provides its own contribution to the correct and timely application of the aforementioned principles. The application of these principles must also be monitored and supervised by the Privacy Officer.

7.3. Data Protection Impact Assessment (DPIA)

When a type of Processing presents a high risk for the rights and freedoms of the Data Subjects (e.g. the use of new technologies), the Data Controller carries out, before proceeding with the Processing, an assessment of the impact of the same on the Personal Data with reference the aforementioned rights and freedoms.

This assessment must be performed in all cases in which an initial analysis leads to the belief that the Processing presents specific risks based on the type of Data processed, the characteristics and methods of the Processing, the tools used and the possible repercussions on the rights and the freedoms of the Data Subjects. Furthermore, once the assessment has been carried out, it will still be necessary for it to be periodically updated in order to review the results also in consideration of the changes that have taken place in the Processing. The assessment takes into consideration the entire life cycle of the Personal Data, from collection to cancellation and takes into account any specific elements required by the particular context in which the Processing takes place (e.g. Profiling, children's data, etc.) as well as the Privacy Provisions.
However, the impact assessment is carried out in the following cases:

- Automated processing, including profiling, on which automated decisions are based that have legal effects or similarly significantly affect the Data Subjects;
- Processing, on a large scale, of Particular Data that present a high risk to the rights and freedoms of the Data Subjects;
- systematic large-scale surveillance of an area accessible to the public;
- Processing of Data subject to impact assessment requested by the Supervisory Authority through lists made public by the same Authority.

In detail, this data protection impact assessment includes:

- a clear and exhaustive description of the Processing required and the purposes of the Processing;
- an assessment of the necessity and proportionality of the Processing in relation to the purposes;
- an assessment of the risks to the rights and freedoms of the Data Subjects;
- a list of the guarantees, Security Measures and mechanisms to guarantee the protection of Personal Data that the Data Controller considers necessary to adopt in order to demonstrate the compliance of the Processing with the requirements of the Privacy Provisions.

7.4. Data Breach

Any event that involves - accidentally and/or unlawfully - the loss of confidentiality, integrity and/or availability of Personal Data processed by the Data Controller and represents a breach ("Data Breach") which, in certain cases, could cause tangible and/or intangible damage to the Data Subjects.
By way of example, but not limited to, cases of a possible breach of Personal Data may consist of:

- loss of Data (whether in electronic or paper format) understood as the ascertained impossibility of restoring the same. By way of example: fire/flooding of paper archives;
- unauthorised access to the Data (computer systems or paper archives) understood as a violation of the confidentiality of the Data contained in the computer systems or archives. For example: a cyber attack through the exploitation of system vulnerabilities or the abusive use of authentication credentials; consultation of paper archives to which access is restricted to authorised staff only;
- loss of the integrity of the Data understood as irremediable compromise of the fairness, congruence and consistency of the Data. By way of example: compromise resulting from unauthorised modification of Data, human error or IT incidents;
- disclosure or disclosure of Data to unauthorised third parties, even if not identified, for example by e-mail or verbally.

For these reasons, the ERG Group has adopted the "Data Breach Management" Procedure for the correct management of security incidents relating to Personal Data, which is referred to in full.

The rules for ensuring compliance with the principles indicated in the Privacy Provisions in case of a Data Breach can be summarised as follows:

- how to identify an event that may constitute a breach;
- methods and cases of reporting to the Data Controller and the Privacy Representative through the Data Processor.

- assessment of the event that occurred;
- any communication to the data subjects;
- methods of reporting within 72 hours of the event to the Supervisory Authority in case the assessments carried out reveal a probable risk to the rights and freedoms of the Data Subjects.

7.5. Rights of data subjects

In compliance with the rules on the processing of Personal Data, the ERG Group, as Data Controller, guarantees and arranges the measures to ensure the exercise, by the Data Subject, of the following rights:

- right of access: the right to obtain from the Data Controller confirmation as to whether or not the Personal Data is being Processed and, in this case, to obtain information in this regard;
- right of adjustment: the right to obtain the adjustment of inaccurate Personal Data and/or the integration of incomplete Personal Data;
- right to erasure: the right to obtain that the Personal Data processed be erased for legitimate reasons;
- right to limitation of Processing: so that the Data processed by the Data Controller are marked in such a way as to limit their processing in the future;
- right to data portability: the right to obtain the receipt of Personal Data, or the transmission of the Data to another Data Controller, in a structured format, commonly used and readable by an automatic device;
- right to object: the right to object to the Processing of the Data at any time, unless there are legitimate reasons to proceed with the Processing that are prevalent (for example, for exercise or defence in court);
- automated decision-making process: the right not to be subjected to a decision based solely on automated processing, including profiling.

Before checking, it is essential to ascertain the identity of the interested party through a copy of a valid identity document.
If the request comes from a person acting on behalf of the Data Subject, it is necessary to check:

- the mandate signed by the Data Subject;
- the identity of the Data Subject and the delegated party.

If the request concerns access to the data of a deceased person, it is necessary to identify the applicant and ensure that it is an heir, or in any case, a person entitled to exercise the right.

The ERG Group has set up a special mailbox for the receipt of requests relating to the exercise the rights recognised rights of the Data Subject.
The management of requests is the responsibility of the Compliance 231 & Privacy organisational unit, which:

- oversees the channels dedicated to the receipt of these requests (e.g. casellaprivacy@erg.eu);
- requests assistance from the organisational units involved in the processing of data of the interested parties (e.g. HR, ICT, IR & Communication);
- provides feedback to the request.

The response to the Data Subject must be provided without undue delay and, in any case, at the latest within one month of receipt of the request.
This deadline may be extended by two months, if necessary, taking into account the complexity and number of requests. In this case, the Company must inform the Data Subject of this extension, and of the reasons for the delay, within one month of receipt of the request.

Finally, the Data Subject has the right at any time to lodge a complaint with the Supervisory Authority.

7.6. Processing of Personal Data by Third Parties

Personal Data may be processed in the name and on behalf of the Data Controller by Third Parties (suppliers, business partners or consultants) appointed to carry out activities that involve the use of the Data Controller's Personal Data. These activities can be performed only after subscription of a specific contract that must have the characteristics set out in Art. 5.2 of the Model.

The ERG Group has defined a standard for the appointment of a Data Processor. If Third Parties propose changes to the standard or propose different agreements, it is necessary to involve the Compliance 231 & Privacy organisational unit in order to review them in order to ensure compliance with the measures necessary to protect the Personal Data processed by the Group.

7.7. Transfer of Personal Data

In carrying out its activities, the ERG Group may transfer Personal Data to non-EU countries.
The transfer is only permitted if at least one of the following conditions is met:

- the transfer is carried out to countries that guarantee an adequate level of protection of the Personal Data and that have been identified by the European Commission;
- the Data Subject has given his/her express consent;
- the transfer is necessary for the execution of obligations derived from a contract of which the Data Subject is a party or to fulfil, before the conclusion of the contract, specific requests of the Data Subject, or for the conclusion or for the execution of a contract stipulated in favour of the Data Subject;
- the transfer is necessary to assert or defend a right in court, provided that the Data is transferred exclusively for these purposes and for the period strictly necessary for its pursuit;
- the transfer is carried out for Third Parties through a contract that includes the standard contractual clauses for the protection of Personal Data defined by the Privacy Provisions.

7.8. Inspections by the Supervisory Authority

Competent Supervisory Authorities may conduct inspections at the Group Companies in order to verify the effective application by the latter of the Privacy Provisions.
During these inspections, ERG will adopt the precautions and safeguards envisaged by the Internal Regulations regarding the management of inspections (Procedure “Management of inspections”).
In general, in case of contact between the Staff and officers representing the offices of the Supervisory Authority, the person in charge of the person involved and the Privacy Officer must be notified immediately.
Documents or information related to the Processing may be delivered to the inspectors only with the authorisation of the Privacy Officer, who must attend the inspection visit.
The Privacy Officer supports the Privacy Representative in any interaction with the Supervisory Authority, while facilitating access to the necessary information and cooperating with it.

8. IMPLEMENTATION AND UPDATING OF THE MODEL

The Privacy Officer, with the support of the *Compliance 231 & Privacy* organisational unit, is responsible for:

- checking the adoption of the Model by ERG Group Companies.
- the updating of the Model, also following any reports from the organisational units and/or any anomaly or difficulty with regard to the application of the Model and the related Privacy Provisions.
- providing advice to Staff of the ERG Group regarding any doubt or topic concerning application of the Model.

The Model is a constantly evolving document, which must be updated when there are regulatory changes regarding the protection of Personal Data or organisational changes within the ERG Group that involve changes to the Internal Regulations and instructions contained in the Model or in the

Privacy Organisation, as well as in the cases in which the Group changes its technical and organisational Security Measures.

For anything not expressly regulated within the Model, reference is made to the Internal Regulations, even when different from those mentioned in the Model, as these documents, subject to constant updating, are an integral and substantial part of the latter.

9. REPORTING OF VIOLATIONS AND WARRANTIES

The Companies of the ERG Group guarantee the possibility of reporting breaches of the Privacy Provisions and of this Model.

In particular, if a person included among the Personnel of the ERG Group, Third Parties, and all those who operate, in Italy and abroad, on behalf of or for the ERG Group has reasonable suspicion that a Data Breach has occurred or may occur, or any breach of the Model, they must report it.

- to the Compliance 231 & Privacy organisational unit using one of the following channels:
  - e-mail: casellaprivacy@erg.eu;
  - ordinary mail, by writing to *Compliance 231 & Privacy* – via De Marini, 1 – 16149 Genova; or
- via the ERG Group's whistleblowing platform, which can be accessed from https://erg.integrityline.com/frontpage, using any browser, including mobile devices. The sending, receipt and management of Whistleblowing Reports (including the protections reserved to the whistleblower) are governed by the "Whistleblowing" Guidelines adopted by the ERG Group.

10. DISCIPLINARY SYSTEM

The commission of acts in breach of the Model as well as, more generally, the breach of the Privacy Provisions, may expose the Data Controller to different types of liability and consequent sanctions (of an administrative and/or criminal nature).

These breaches constitute a default of contractual obligations and Internal Regulations and may give rise to the initiation of proceedings for the imposition of sanctions against the relative perpetrators.

Specifically:

- Employees of the ERG Group are subject to the sanctions required by the National Collective Labour Agreement (or equivalent document) applicable pro tempore, while the same sanctions will be applied by the Human Resources organisational unit;
- the members of the management and control bodies are subject to removal from office as resolved by the relevant shareholders' meeting;
- collaborators and Third Parties are subject to the sanctions provided for in the contracts stipulated with the ERG Group Companies and may come to the suspension and, in the most serious cases, to the termination of the contractual relationship.

In all cases, the penalty must be commensurate with the liability level of the party involved and the intentionality and the seriousness of the conduct and must be without prejudice to the guarantee of the adversarial procedure be applied regardless of whether proceedings were initiated by Monitoring Authorities.

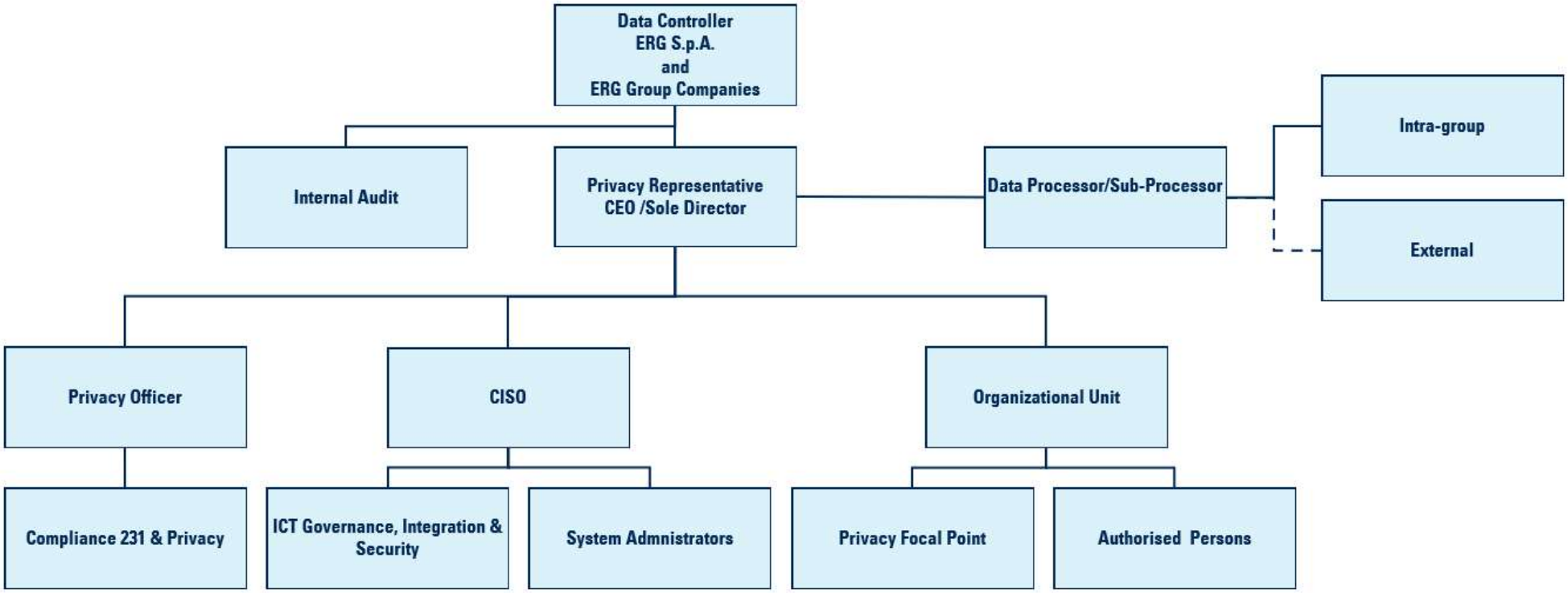
11. DISCLOSURE, COMMUNICATION AND TRAINING

The Model is disclosed, through the Group's internal (e.g. company intranet) and external communication channels (website), to all the People of the ERG Group, to the Relevant Third Parties, to the stakeholders and to the other parties that have relations with the Group.

The Group prepares and implements training plans dedicated to the Processing and protection of Personal Data, the tools to prevent Data Breaches, the contents of the Model and the Privacy Provisions, so as to ensure the dissemination and correct understanding of the principles expressed

in the Model and raise awareness among ERG Group Staff.

ANNEX 1: ERG GROUP PRIVACY ORGANISATION



With reference to intra-group services, some ERG Group companies act as Data Processors or Sub-Processors.