Standard di Compliance

Data Protection

ITH-STC-071-R01
Issue date: 30/06/2021
Date effective: 30/06/2021

Written	COMPLA	ORG&DT	
Verified	ALESOC	HRO	SECUR
Approved	CEO		
Elements of Compliance	**GDPR**		

Chronology of Reviews

- Rev. 01
- Rev. 00
  Document repealed:
  - Procedure ITH-STC-056-R00 "Compliance pursuant to Legislative Decree 196/2003: Personal data protection code", issued with Circular of CEO of 7 December 2017

For the purposes of this document, the terms and definitions available in the "Glossary" section found on the company Intranet apply

Any regulatory references are detailed in the "External References" section available on the company Intranet

Any printed copies of the document are not checked and revised.
Before use it is necessary to check that the document is up-to-date compared with the original in force on the company's intranet and internet site.

CONTENTS

1. ABSTRACT

The European legal framework on personal data protection has been heavily revised by (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" (hereinafter, the "Regulation" or "GDPR"). The Regulation is applicable from 25 May 2018.

The Regulation mainly deals with the protection of natural persons and the free movement of personal data.

The Regulation repealed the previous privacy Directive ("Directive 95/46") and proposes significant changes and requirements to be complied with, at the same time providing continuity with the regulation previously in force.

At national level it is in force the Decree Law n. 196/03 "Personal data protection code" and subsequent amendments and additions, in particular by Decree Law n. 101/2018, after the Regulation came into force.

The Italgas Group recognises that the correct management of personal data is a fundamentally important value and therefore intends to pay the utmost attention to the protection of the personal data collected and processed as part of the company's activities.

Following regulatory intervention by the European Legislator, the Italgas Group has reviewed and updated its personal data Governance system, defining a Data Protection Organisational Model (hereinafter "Data Protection Organisational Model" or "Organisational Model for data protection") inspired by the requirements of the Regulation.

This document aims to define the key points on which the Data Protection Organisational Model of Italgas and its direct and indirect subsidiaries is based, identifying the key figures of the privacy organisation chart and defining the roles and responsibilities in accordance with the Regulation, Guidelines, recommendations and best practices of the European Committee for Data Protection (which replaced, as of 25 May 2018, the c.d. Article 29 Working Party[1]), as well as the provisions of the Data Protection Authority (hereinafter the "Authority"). The Data Protection Organisational Model was approved by the Board of Directors on 7 May 2018, after consulting the Control and Risk Committee and the Board of Statutory Auditors.

The representatives indicated by Italgas on the corporate bodies of affiliates, consortia and joint ventures promote the principles and contents of the Data Protection Model within their areas of responsibility.

2. DEPARTMENTS INVOLVED

Department Mentioned in this document	Organisational Unit
Human Resources Department	Human Resources & Organization (HRO)
Legal Department	Legal, Corporate and Compliance Affairs (ALESOC)
Organisation Department	Organisation & HR Digital Transformation (ORG&DT)
Staff Administration Department	Staff Administration (AMMPER)

[1] The Working Party, set up pursuant to art. 29 of directive 95/46, is an advisory and independent body made up of representatives of the personal data protection authorities designated by each Member State and the EDPS (European Data Protection Supervisor), as well as a representative of the Commission. The chairman is elected by the Working Party from within and has a two-year term of office, renewable once.

3. COMPLIANCE PRINCIPLES

3.1 Personal data and processing

3.1.1 Personal data processing

Personal data **processing** consists of any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.1.2 Personal data

Personal data means any information relating to an identified or identifiable natural person ("**Data Subject**"). In light of the Regulations, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

As part of a broader definition of personal data, the Regulation identifies particular categories of personal data in relation to which precautions should be taken to ensure their protection:

- "data concerning health" (under art. 4 no. 15 GDPR): personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
- "biometric data" (under art. 4 no. 14 GDPR): personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- "genetic data" (under art. 4 no. 13 GDPR): personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- "data relating to criminal convictions and offences," namely data relating to criminal convictions and offences or related security measures (under art. 10 GDPR). These circumstances however are very limited and restricted to the cases required by the regulations (that is, personal data suitable for revealing the measures set out in article 3, subsection 1, letters a) to o) and r) to u), of Presidential Decree No. 313 of 14 November 2002, concerning criminal records, the registry of administrative sanctions connected to a crime and relative pending charges, or the status of defendant or suspect pursuant to articles 60 and 61 of the Code of Civil Procedure).

Personal data is not considered to be anonymous data, or data that from the time of its collection/origin or following processing, cannot be associated with an identified or identifiable Data Subject.

3.1.3 The key principles applicable to the processing of personal data

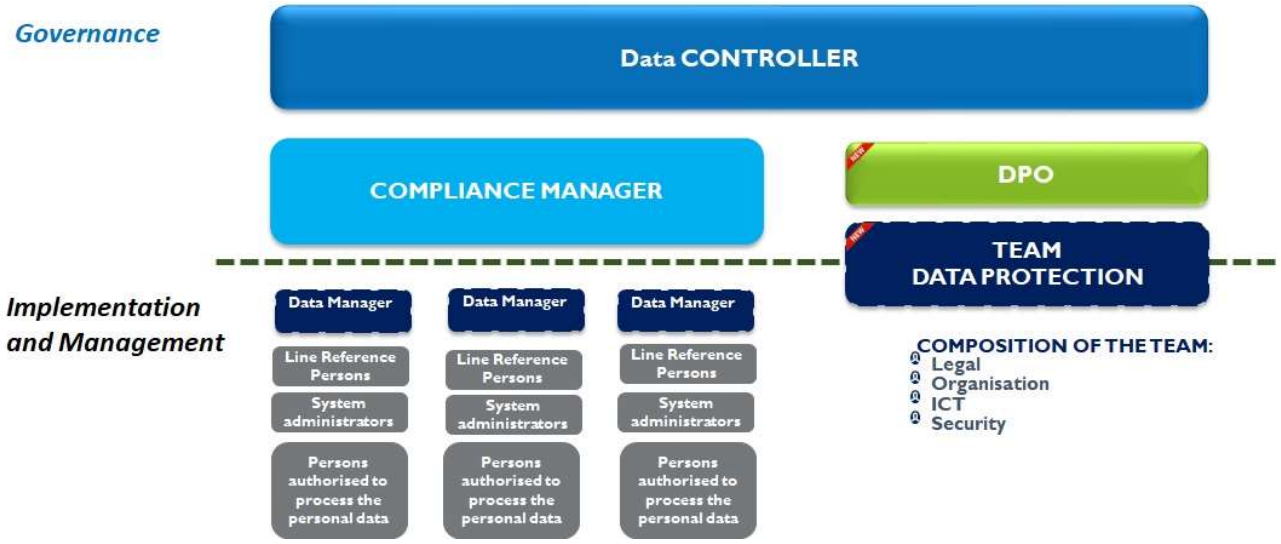
All data processing must be carried out in compliance with the key principles of the regulations on personal data processing, thereby meaning the Regulation, including the underlying recital and the Guidelines of the Article 29 Working Group, current national legislation, including the measures issued by the supervisory authority, where applicable, and best practices, as defined by the European Committee for data protection.

In particular, the processing will be carried out in compliance with the principles set out in articles 5 and 25 of the GDPR as per the attachment (Annex 1).

3.2 The Data Protection Organisational Model

Italgas has defined a Data Protection Organisational Model based on the provisions of the Regulation, as well as the Guidelines of the Article 29 Working Group and the guidelines of the Authority.

The image below shows the roles of the data protection organisation chart.



3.2.1 Key figures of the Data Protection Organisational Model: roles and responsibilities

3.2.1.1 Data Controller

The Data Controller of the personal data is identified as the legal person in whose interest the processing is carried out and who determines the purposes of such treatment (namely Italgas or another direct or indirect subsidiary of Italgas).

The Data Controller is responsible for decisions on the purpose, the methods of processing personal data and the tools used, including the security profile.

The Data Controller is also responsible for ensuring compliance with data protection legislation.

3.2.1.2 Data Protection Officer

The Data Protection Officer, (hereinafter, "Data Protection Officer" or "DPO") is the **natural person** appointed by the Data Controller whose task is to support, coordinate and collaborate with all the company's organisational departments in the management of data protection issues and to monitor compliance with the applicable regulatory requirements and Data Controller policies.
The DPO performs an information and advisory role regarding the main obligations deriving from the Regulation, providing, where requested, opinions and indications on the conduct, evaluation and follow-up as regards the data protection impact assessment (or DPIA).
The DPO cooperates with the Authority in the case of inspections and acts as the contact point for requests made by data subjects in exercising their rights.

The following tasks and duties are assigned to the DPO[2]:

a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to the Regulation and to other Union or national data protection provisions;

b) to monitor compliance with the Regulation, with other Union or national data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

[2] Pursuant to art. 39, paragraph 1 of the Regulations.

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to article 35 of the Regulation;

d) cooperate with the supervisory authority[3];

e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the Regulation, and to consult, where appropriate, with regard to any other matter.

To supplement the tasks described in article 39, paragraph 1, of the Regulation, the DPO is also assigned the following tasks and duties:

a) promote the data protection culture within the company;

b) support the assessment of the data protection aspects of each new project that has or could have an impact on personal data protection in light of the Privacy by Design and Privacy by Default principles (see Annex I), in compliance with company policies on this matter;

c) promote and coordinate Personal data training activities for all employees, with particular attention to the top management figures identified in the model, collaborating in the definition of content and of the training plan;

d) monitor the inclusion of adequate contractual clauses on Personal data protection in the contracts in use;

e) act as a point of contact for the data subjects, for all issues concerning the processing of their data, including the exercise of rights deriving from the Regulation;

f) on an annual basis, promote the updating of the processing Register and check that it is updated;

g) support the Data Controller with the assessment of any data breaches to check if the breach presents a high risk for the rights and freedoms of the data subject and with the consequent notification to the supervisory Authority and any communication to the data subjects, in compliance with company policies;

h) with the support of the Legal Department, monitor the laws or other standards concerning data protection that have an impact on the processing of personal data, promoting internal communication campaigns aimed at updating the organisational departments involved.

From time to time the Data Controller may assign the DPO additional tasks and duties, as long as they are compatible with the role.

The Data Controller shall ensure that the DPO does not receive any instructions regarding the exercise of the tasks referred to in art. 39 of the Regulation.

The contact details of the DPO are published on the website and included in the privacy information notice; they are also made available to the company organisation by publication on the company Intranet.

In addition, the contact details of the DPO are communicated to the supervisory Authority.

In order to facilitate communication flows to the DPO a dedicated channel has been set up in the form of the email address dpo.gdpr@italgas.it.

3.2.1.2.1 DPO information flows

In order to ascribe the DPO suitable capacity to retrieve the information and therefore make the actions of this figure effective with regard to the company organisation, the information flows from and to the DPO are defined both through this Compliance Standard and, thereafter, in specific internal organisation documents.

[3] The supervisory authority (for the Italian State this is the Italian Data Protection Authority), is the body responsible for handling any complaints it receives or any infringements of the European Regulation and national laws on data protection, if the object is limited to an establishment in its Member State or has a substantial impact on the data subjects exclusively in its Member State.

In order to ensure full autonomy and independence in the performance of the relative duties, the DPO reports to the Board of Directors and the Control Bodies at least once a year on compliance with the Regulation and with company policies, implementation of the Data Protection Organisational Model, the results of the monitoring activities carried out and any actions to implement and improve the model.

In particular, the information flows mentioned above are organised as follows:

i. continuously with regard to the Control Bodies and the Board of Directors, in all circumstances in which it is considered necessary and/or appropriate to implement the obligations laid down in the Regulation, providing all relevant and/or useful information for the correct fulfilment of the provisions of the Regulation;

ii. in a written report to the Board of Directors, at least once a year, on the activities carried out, the requests of the data subjects, the requests of the supervisory authority, and the suggestions on the corrective measures to be adopted to do away with any misalignments found.

The DPO may be summoned by the Board of Directors at any time and, in turn, may request to be heard by the BoD if an opportunity arises to report on questions pertaining to the operation of the Data Protection Organisational Model, data processing and/or compliance with the Regulation.

The DPO participates, upon invitation, at the meetings of the Control and Risk Committee and the Supervisory Body, at least once a year, to report on the state of implementation of the Regulation, the Organisational Model and the Data Controller's policies on personal data protection.

3.2.1.3 Compliance Manager

The Data Controller, through a Board of Directors resolution, identifies the Compliance Manager from among natural persons holding management roles at the Company.

Given the complexity of the company organisation, within the Group the Compliance Managers identified are: the Head of the Human Resources Department for Italgas and the Chief Executive Officers for the direct or indirect subsidiaries[4].

The Compliance Manager, with the necessary powers granted by the Data Controller, has the task of ensuring that any processing undertaken by the company is performed in compliance with the Regulation and with current legislation on personal data protection.

Moreover, the Compliance Manager is required to support the Data Controller in the definition of company policies on data protection and ensure the corporate documentation is compliant with the requirements of the Regulation, constantly monitoring the evolution of the reference regulatory framework in coordination with the DPO and with the operational support of the Legal Department.

The tasks and responsibilities attributed to this figure are, by way of example:

- ensure compliance with the Regulation, current legislation on Personal Data Processing, the Data Protection Organisational Model, as well as the policies of the Data Controller on data protection;
- support the Data Controller in the definition of company policies on data protection;
- monitor, with the support of the Legal Department, the evolution of the regulatory framework of reference and data protection practices;
- appoint the Data Managers, chosen from among persons who, given their experience, ability and reliability, provide adequate assurance of full compliance with the current provisions regarding Processing, including the security profile,
- define the roles and duties of the Data Managers;
- define, in coordination with the Data Managers, the role and duties of the Reference Persons;
- ensure the corporate documentation is compliant with the requirements of the Regulation (for instance information and contracts) and the Data Protection Organisational Model.

[4] It is understood that the Boards of the direct or indirect subsidiaries of Italgas must appoint a DPO and a Compliance Manager.

3.2.1.4 Data Protection Team

The Data Protection Team has been set up and tasked with assisting and supporting all company roles involved in the processing.

The members of the Data Protection Team have specific knowledge in the following areas: Legal, Information Technology, Business security and Organisation and Processes.

The Team members are identified by the Organisation Department through a specific organisational tool.

The Data Protection Team carries out the following tasks and duties:

- it provides support with fulfilling the requirements laid down in the Regulation and company regulations (e.g. updating the records of processing activities and operational documentation relevant for data protection purposes, carrying out a data protection impact assessment for high risk processing, etc...).
- it provides support with identifying and implementing the technical and organisational measures;
- it collaborates with the DPO in checking the compliance of activities pertaining to Personal Data protection with respect to regulatory requirements with particular attention to the process of assessing anomalous events that could be considered data breaches, cooperating with activities concerning notification of the Authority, and if applicable the Data Subject, and the subsequent activities required by legislation;
- in collaboration with the HRO organisational structure, the Legal Department and the DPO, it assesses the company training requirements regarding data protection and defines an adequate training plan.

3.2.1.5 Data Managers

Data Managers are the natural persons in charge of running the company's organisational departments involved in the processing and they have the task of supervising the performance of operations carried out by the Reference Persons and Data Processing Operators who operate within their organisational structure, ensuring compliance with personal data processing legislation.
The Data Managers are chosen among persons who, given their experience, ability and reliability, provide adequate assurance of full compliance with the current provisions regarding Processing, including the security profile[5].

The roles and duties of the Data Managers are analytically specified in writing by the Compliance Manager who proceeds with their designation.

The Organisation department submits to the Data Managers the letter of appointment, signed by the Compliance Manager, to be signed in acceptance. The signed letter is sent to the Staff Administration Department for filing in the employee's personal folder. The Organisation department prepares/updates the list containing the names of the Data Managers and makes it available on the company Intranet.
This list is kept up-to-date by the Organisation department and made promptly available, in case of need, to the DPO (e.g. following a request by a Data Subject).

3.2.1.6 Line Reference Persons

Line Reference Persons are the natural persons who perform a support and connection function, assisting the Data Manager in performing the personal data processing actions.

The Organization Department, in agreement with the Data Managers, prepares/updates the list containing the names of the Line Reference Persons and makes it available on the company Intranet.
This list is kept up-to-date by the Organisation Department and made promptly available to the DPO if necessary.

[5] In line with the provisions already established for other corporate systems (e.g. SCIS, 231 etc.…)

3.2.1.7 System Administrators[6]

Given the technical aspects, System Administrators play an extremely delicate role: they design, develop and manage the network infrastructure, servers, software and basic application services, often dealing with the security and protection of data and resources. Moreover, they provide technical and IT support for software and hardware. They support the Data Managers with technical IT aspects in normal operating activities.

Persons having the following requisites may be chosen as System administrators:

- IT skills, including in relation to issues regarding security, for example considering the training, professional experience acquired, etc.;
- compliance with regulatory and company provisions regarding the processing of personal data.

The System Administrator is individually chosen by the relevant Data Manager in compliance with the above criteria, by letter signed by the latter.

The System Administrator signs and dates the letter in acknowledgement.

The signed letter, with the analytical list of the permitted operating areas according to the authorisation profile assigned, is sent to the Staff Administration Department and the Staff Management Department for filing in the employee's personal records and to the DPO for the processing/update of the list containing the identification details of the natural persons appointed as System Administrators.

3.2.1.8 Persons authorised to process the personal data

The persons authorised to process the personal data are natural persons in charge of processing actions acting under the responsibility of the Data Managers and in compliance with the instructions received from them. In practical terms, they perform processing actions for the personal data contained in databases and in the company's paper files, in the exercise of the duties entrusted to them.

3.3 Consequences of non-compliance with data protection regulations

The organizational and regulatory system of the Italgas Group defines rules and processes and ensures their implementation and traceability in accordance with the accountability principle.

All persons authorised to process personal data receive instructions for the processing, according to their function and the context in which they operate; in addition, they are informed of the tools to be used to report any data breaches.

Failure to comply with the instructions for data processing, this Compliance Data Protection Standard or, more generally, the company rules on personal data protection leads to the opening of a disciplinary procedure, which could result in the adoption of measures commensurate with the severity of the infringement.

In case of non-compliance with the Data Protection regulations, the Data Manager:

- performs an analysis of events,
- defines and implements appropriate corrective actions,
- communicates the corrective actions defined to the DPO, which monitors their implementation.

[6] System Administrators are the persons in charge of managing and maintaining a data processing system or its components, as defined by the Italian Data Protection Authority Measure of 27 November 2008 ("Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator").

4. CONSERVATION OF DOCUMENTATION AND RESPONSIBILITY FOR UPDATES

All the work documentation, arising from the application of this document, shall be conserved by the relevant Departments, in accordance with the timing and procedures laid down by the Italgas Enterprise System.

The updating of the document in question and the relative disclosure shall be ensured by the procedures laid down by the Italgas Enterprise System.

The Company, as part of a vertically integrated company, is subject to the separation obligations functional pursuant to the Functional Unbundling Integrated Text ("Testo Integrato Unbundling Funzionale" or "TIUF") adopted by the Authority Regulation for Energy, Networks and the Environment ("ARERA"), with resolution no. 296/2015/R/com. It is also subject to the accounting separation obligations pursuant to the Integrated Text Unbundling Contabile ("Testo Integrato Unbundling Contabile" or "TIUC") pursuant to the ARERA Resolution of 24 March 2016, no. 137/2016/R/com.

This procedure is always applied in compliance with the obligations and objectives of the unbundling discipline. In particular, Commercially Sensitive Information and information related to distribution infrastructure, are treated in accordance with the procedure Access to commercially sensitive information and its annexes.

5. LIST OF ANNEXES

Annex		Responsible for Updates
I	Key principles applicable to the processing of personal data	Legal Department