



Compliance Standard

Data Protection

Document Code: Enaon-STC-015-R00

Issue Date: 22/07/2024

Drafted

DPO

Verified

COMPLA

ORG

CERTF

SECUR&RE

LEGAL

HRO

Approved

CEO

Elements of Compliance

GDPR

Revision history

- Rev. 00 (first issue)

The Company Internal Document Library is the official source of the documents in force. When using printed documents, it is always necessary to check that they are up to date with the original in force on the Company Internal Document Library.

The Company, where the conditions are met, is required to comply with the unbundling legislation in all its forms. In particular, it is subject to accounting separation obligations and the management of Commercially Sensitive Information must take place in compliance with the provisions of specific regulations.

INDEX

1	ABSTRACT	3
2	FUNCTIONS INVOLVED	4
3	COMPLIANCE PRINCIPLES	4
3.1	Personal data and processing	4
3.1.1	Personal data processing	4
3.1.2	Personal data.....	4
3.1.3	The key principles applicable to the processing of personal data	5
3.2	The Data Protection Organizational Model	5
3.2.1	Key figures of the Data Protection Organizational Model: roles and responsibilities	5
3.2.1.1	Data Controller	5
3.2.1.2	Data Protection Officer.....	6
3.2.1.3	Privacy Compliance Manager.....	8
3.2.1.4	Data Protection Team.....	8
3.2.1.5	Data Managers	9
3.2.1.6	Line Reference Persons	10
3.2.1.7	System Administrators.....	10
3.2.1.8	Persons authorised to process the personal data	10
3.3	Consequences of non-compliance with data protection regulations.....	11
4	CONSERVATION OF DOCUMENTATION AND RESPONSIBILITY FOR UPDATES.....	11
5	ANNEXES/ FORMS LIST	11

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The Regulation repealed the previous privacy Directive (“Directive 95/46”) and proposes significant changes and requirements to be complied with, at the same time providing continuity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 the national level, the law 4624/2019, prescribes measures for implementing the GDPR. It also facilitates the transposition of Directive (EU) 2016/680 from the European Parliament and Council dated April 27, 2016, among other provisions.

Enaon 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, Enaon has reviewed and updated its personal data Governance system, defining a Data Protection Organizational Model (hereinafter “Data Protection Organizational Model” or “Organizational Model for data protection”) inspired by the requirements of the Regulation.

This document aims to define the key points on which the Data Protection Organizational Model of Italgas and its direct and indirect subsidiaries – including Enaon - is based, identifying the key figures of the privacy organization 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 Party¹), as well as the provisions of the Hellenic Data Protection Authority (hereinafter the “Authority”). The Data Protection Organizational Model was approved by the Board of Directors on 22/07/2024.

The representatives indicated by Enaon 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.

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.

2 FUNCTIONS INVOLVED

FUNCTION MENTIONED IN THE DOCUMENT	ORGANIZATIONAL UNIT
HR Management Unit	Human Resources & Organization (HRO)
Legal Affairs Unit	Legal Services Division
Organization Unit	Human Resources & Organization (HRO)

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, organization, 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 Regulation, 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.

Special Categories of Personal data

The Regulation identifies special categories of personal data, the processing of which is performed strictly under specific conditions mentioned in Article 9 of the Regulation². In addition, due to the highly sensitive nature of special categories of personal data, Enaon establishes stricter technical and organizational measures for their protection.

Such data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning a natural person's sex life or sexual orientation, Moreover, include genetic data, biometric data (processed for the purpose of uniquely identifying a natural person), data concerning health, as specified below:

- “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

² Examples of the Art. 9, GDPR conditions include:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Enaon or of the data subject in the field of employment and social security and social protection law,
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity,
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

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.

Moreover, Enaon may also process personal data relating to criminal convictions and offences. In cases where such processing is necessary, Enaon ensures that it will be lawful and carried out based on the relevant mandates of GDPR (Art. 10).

Anonymous data

Data which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, are not considered personal data, therefore, the principles of data protection do not apply to it.

3.1.3 The key principles applicable to the processing of personal data

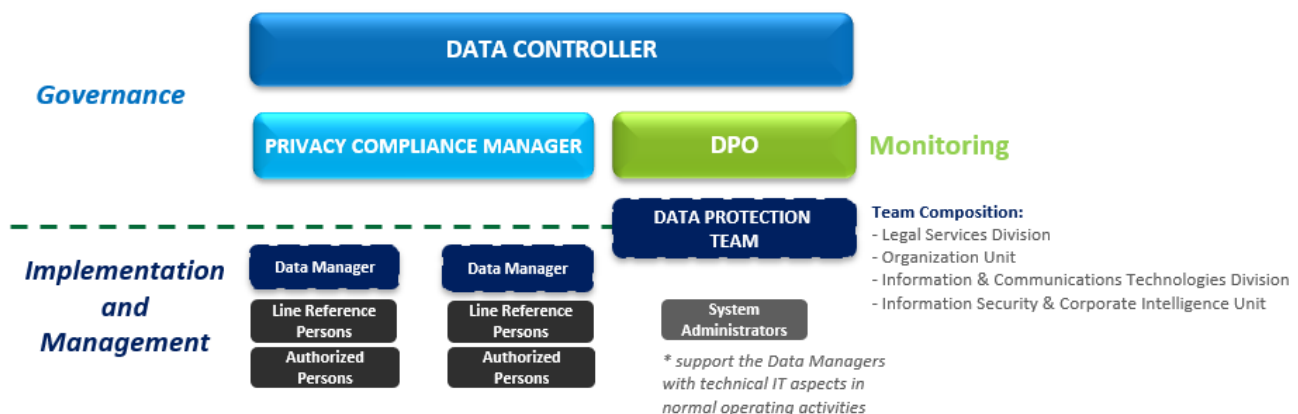
All data processing must be carried out in compliance with the key principles of the regulations on personal data processing, thereby meaning the Regulation, including the underlying recital and the Guidelines of the Article 29 Working Group, current national legislation, including the measures issued 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 Organizational Model

Enaon has defined a Data Protection Organizational 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 organization chart.



3.2.1 Key figures of the Data Protection Organizational 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 – including Enaon).

The Data Controller is responsible for decisions on the purpose, the methods of processing personal data and the tools used, including the data 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 organizational divisions 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 DPO³:

- 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;
- 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) to cooperate with the supervisory authority⁴;
- 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) to promote the data protection culture within the company;
- b) to 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) to 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) to monitor the inclusion of adequate contractual clauses on personal data protection in the contracts in use;
- e) to 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, to promote the updating of the Records of Processing Activities and to check that it is updated;

³ Pursuant to art. 39, paragraph 1 of the Regulations.

⁴ The supervisory authority (for the Greek State this is the Hellenic 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.

- g) to support the Data Controller with the assessment of any data breaches, in order to ascertain 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 (if needed), in compliance with company policies and the regulatory framework;
- h) with the support of the Legal Services Division, to 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 organizational divisions involved;
- i) to support the Data Controller in the definition of personal data protection framework (including policies, procedures and instructions) and ensure that the framework is compliant with the requirements of the Regulation (for instance information and contracts) and the Data Protection Organizational Model;
- j) to support the competent Data Manager of Enaon in assessing third parties (e.g. service providers, suppliers, consultants, etc.) which process personal data on behalf of Enaon in order to identify any risks arising from such processing and monitor the implementation of the relevant plan for the mitigation of the identified risks.

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 organization 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@ena-on.gr.

3.2.1.2.1 DPO information flows

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

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 Organizational 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 organized 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 Organizational Model, data processing and/or compliance with the Regulation.

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

A flow of communication is established between the DPOs of the Italian companies and of the Greek companies of Italgas Group where a need arise for discussion on specific topics or for aspects regarding synergies and for sharing of information.

3.2.1.3 Privacy Compliance Manager

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

Given the complexity of the company organization, within the Group the Compliance Managers identified are: the Head of the Human Resources and Organization for Italgas and the Chief Executive Officers for the direct or indirect subsidiaries - including Enaon⁵.

The Privacy 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 Privacy 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 Division.

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

- manage and monitor the budget of expenditure required for the implementation of the Company's personal data protection strategy;
- ensure compliance with the Regulation, current legislation on Personal Data Processing, the Data Protection Organizational Model, as well as the policies of the Data Controller on data protection;
- support efforts and initiatives concerning the personal data protection;
- support the Data Controller in the definition of company policies on data protection;
- monitor, with the support of the Legal Division and the DPO, 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;
- ensure the corporate documentation is compliant with the requirements of the Regulation (for instance information and contracts) and the Data Protection Organizational Model.

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 Organization and Processes.

⁵ It is understood that the Boards of the direct or indirect subsidiaries of Italgas must appoint a DPO and a Compliance Manager.

The Team members are identified by the Organization Unit through a specific organizational tool.

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

- 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).
- provides support with identifying and implementing the technical and organizational measures;
- 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 organizational structure, the Legal Division and the DPO, it assesses the company training requirements regarding data protection and defines an adequate training plan.

A flow of communication is established between the Data Protection Teams of the Italian companies and of the Greek companies of Italgas Group where a need arise for discussion on specific topics or for aspects regarding synergies and for sharing of information.

3.2.1.5 Data Managers

Data Managers are the natural persons in charge of running the company's organizational divisions involved in the processing and they have the task of supervising the performance of operations carried out by the Reference Persons and persons authorised to process the personal data who operate within their organizational structure, ensuring compliance with personal data processing legislation.

The Data Managers are chosen among persons who, due to their experience, ability and reliability, provide adequate assurance of full compliance with the current provisions regarding personal data processing, including the data security profile⁶.

The roles and duties of the Data Managers are analytically specified in writing by the Privacy Compliance Manager who proceeds with their designation. Indicative tasks that may be assigned to the Data Managers are:

- to communicate, on behalf of the Division, with the DPO for clarifications and questions related to data protection;
- to assess third parties (e.g. service providers, suppliers, consultants, etc.) which process personal data on behalf of Enaon in order to identify any risks arising from such processing and monitor the implementation of the relevant controls, as well as of the plan for the mitigation of the identified risks;
- to ensure that specific time periods for the retention of personal data have been defined on the basis of the respective legal, regulatory, operational and contractual requirements and carry out checks in order to ensure that the defined retention periods are adhered to;
- to define the role and duties of the Reference Persons;
- to monitor the Division's personal data protection practices, as well as the degree of compliance to the data protection framework established by Enaon;
- to ensure the proper implementation and efficiency of technical and organizational measures regarding the personal data processed by the Division;

⁶ In line with the provisions already established for other corporate systems (e.g. SCIS, 23I etc....)

- to maintain the Division's Record of Processing Activities and ensure it is updated at all times, by incorporating any changes to the processing activities of the Division;
- to carry out DPIAs where necessary, along with the support of the DPO.
- to facilitate the proper management of data subject requests related to the processing activities of the Division, along with the support of the DPO, and
- to monitor the implementation of any remediation actions, in the context of periodic compliance assessments.

The Organization Unit submits to the Data Managers the letter of appointment, signed by the Privacy Compliance Manager, to be signed in acceptance. The signed letter is sent to the HR Management Unit for filing in the employee's personal folder. The Organization Unit 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 Organization Unit 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 and in particular in the performance of processing that may present a high risk to the rights and freedoms of natural persons.

3.2.1.7 System Administrators⁷

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 HR Management Unit for filing in the employee's personal records and the 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.

⁷ System Administrators are the persons in charge of managing and maintaining a data processing system or its components.

3.3 Consequences of non-compliance with data protection regulations

The organizational and normative system of Enaon 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 Data Protection Compliance Standard or, more generally, the company rules on personal data protection leads to 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.

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 Divisions, in accordance with the timing and procedures laid down by the Italgas Enterprise System.

5 ANNEXES/ FORMS LIST

Annex/ Form		Responsible for Updating
Annex 01	Key principles applicable to the processing of personal data	Legal Services Division