



PRIVACY GUIDELINES

Document approved by the Board of Directors on 8th May 2018

Table of contents

1. Objective and scope	3
2. Regulatory Framework	3
3. Basis of lawfulness of processing	4
4. Rights of data subjects	5
4.1 Right of access	5
4.2 Right of rectification	5
4.3 Right to erasure (so-called right to be forgotten).....	6
4.4 Right to restriction of processing.....	6
4.5 Right to data portability	6
5. Privacy management system.....	7
5.1 Risk Assessment, Gap Analysis, Remediation Plan and information flows ..	7
5.2 Privacy Impact Assessment.....	7
5.3 Privacy policy.....	8
5.4 Processing Register.....	8
5.5 Security measures	9
5.6 Personal data breaches.....	9
5.7 Privacy by design and by default	10
6. Operational procedures for processing personal data	12
6.1 Documentation archiving	12
6.2 Data retention	12
6.3 Processing of personal data by means of video surveillance systems	13
7. Roles and responsibilities	13
7.1 Personal data controller.....	13
7.1.1 Joint controllers.....	13
7.2 Privacy Compliance Officer	14
7.3 Data Protection Officer	14
7.4 Data Processors	15
7.4.1 (External) data processor.....	15
7.4.2 (Internal) Delegated data processor.....	16
7.4.3 Officer in charge of processing	17
7.5 System Administrator.....	17
8. Operational tools.....	19
9. Training and communication.....	19
10. Responsibility for updating.....	20

1. Objective and scope

The purpose of this Guideline is (i) to define the corporate roles and the obligations to be implemented with regard to the protection of personal data pursuant to Regulation (EU) 2016/679 (hereinafter, the “Regulations”) and (ii) to direct all Snam employees so that the processing of personal data is carried out in compliance with the fundamental rights and freedoms of natural persons and in particular the right to protection of personal data.

This Guideline specifies the actions to be taken in accordance with both national and Community legislation on the processing and protection of personal data, as well as the provisions of the Authority and the relevant interpretation and case law.

This Guideline applies to Snam and to its subsidiaries subject to management and coordination activities and is also brought to the attention of other investee companies in order to promote principles and conduct consistent with those expressed by Snam.

2. Regulatory Framework

The Regulations, which will be directly applicable to all member states from 25 May 2018, stems from specific needs, as indicated by the EU Commission itself, for legal certainty, harmonisation and greater simplicity of the rules concerning the transfer of personal data from the EU to other parts of the world.

In particular, a stricter form of *accountability* of data controllers and an approach that takes greater account of the risks that a given processing of personal data may entail for the rights and freedoms of data subjects have been defined, based on the principle of accountability. In addition, (i) clearer rules on information and consent were introduced; (ii) the basis for exercising new rights was defined; (iii) strict criteria for transferring personal data outside the EU were established; and (iv) strict rules were set for data breaches.

Within the framework of the new regulatory context, Snam, which is aware of the challenges arising from the development of new technologies and taking into account the need to protect personal data, which is increasingly perceived by EU citizens, in line with the provisions of the Code of Ethics, undertakes to protect information relating to its own People and third parties, generated or acquired within and in business relations, and to avoid any improper use of this information. Snam intends to ensure that the processing of personal data carried out within

its structures takes place in compliance with the fundamental rights and freedoms, as well as the dignity of the persons concerned, as provided for by current legislation.

Below is a description of the principles and cornerstones underlying the rules of conduct on privacy that all Snam's People, and those who work for it, are required to comply with.

3. Basis of lawfulness of processing

The processing of personal data is only permitted at Snam if it is lawful. Otherwise, each individual operating in Snam must refrain from carrying out processing operations.

The processing of the personal data of the Data Subject by the Controller is lawful only if it is based on at least one of the following conditions:

- expression of consent by the data subject in an explicit, free, specific, informed, not tacit or presumed manner;
- fulfilment of contractual obligations to which the data subject is a party;
- fulfilment of a legal obligation by the Data Controller;
- performance of a task carried out in the public interest or in the exercise of the public powers assigned to the Data Controller;
- pursuit of a legitimate interest of the Data Controller or even of a third party, unless the interests or the fundamental rights and freedoms of the Data Subject prevail, after having been balanced by the same Data Controller - in implementation of the principle of accountability - between the legitimate interest and the rights and freedoms of the Data Subject;
- safeguard of vital interests¹ of a third party only if none of the above conditions of lawfulness apply.

Within Snam, personal data are processed in accordance with the above conditions and the Data Controller ensures compliance with them.

¹ By way of example, vital interests shall refer to cases where processing is necessary for humanitarian purposes, inter alia, in order to control the development of epidemics and their spread or in cases of humanitarian emergencies, in particular natural and man-made disasters.

4. Rights of the data subject

In accordance with the applicable regulations on the processing of personal data, the Data Controller guarantees and provides tools and measures to ensure appropriate and timely feedback to the data subjects who exercise the following rights under the Regulations:

(i) right of access, (ii) right of rectification, (iii) right to erasure (so-called right to be forgotten), (iv) right to restriction of processing, (v) right to data portability.

The Data Protection Officer (DPO)², in cooperation with DT&T and Global Security & Cyber Defence, is responsible for handling any requests from data subjects.

4.1 Right of access

The Data Controller shall promptly reply to a data subject who has requested confirmation as to whether or not personal data concerning him/herself are being processed and, if so, shall grant access to such data. Access is accompanied by further information on the processing of the data subject's personal data, such as: (a) the purposes of processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the data have been or will be disclosed; (d) the data retention period or criteria used to determine it; (e) the possibility for the Data Subject to request the rectification or erasure of his/her personal data or the restriction of the processing of his/her personal data; (f) the right to lodge a complaint with the Supervisory Authority; (g) the origin of the data collection if not collected directly from the Data Subject; (h) the existence of an automated decision-making process.

In the event of transfer of personal data to a third country or international organisation, the Data Controller shall inform the Data Subject of the guarantees applied in this respect.

4.2 Right of rectification

The Data Subject has the right to obtain from the Data Controller the rectification of inaccurate personal data concerning him/her without undue delay. The Data Controller shall rectify inaccurate personal data or supplement incomplete personal data, including by means of a supplementary declaration provided by the data subject.

² See section 7.3.

4.3 Right to erasure (so-called right to be forgotten)

The Data Controller proceeds to erase the personal data relating to the Data Subject in the cases determined and provided for by the applicable law. By way of example, the cases that could most affect Snam are:

- a) the data are no longer necessary for the purposes for which they were collected;
- b) revocation of consent, if necessary and expressed by the data subject in advance;
- c) unlawful processing (i.e. without consent and without the cases of exemption from consent provided for in paragraph 3 above).

4.4 Right to restriction of processing

Snam, as Data Controller, shall restrict the processing of the personal data of the requesting data subject if the data subject so requests and one of the conditions listed below applies.

- the Data Subject contests the accuracy of the personal data;
- the processing is unlawful and the Data Subject objects to the deletion of the personal data;
- personal data are necessary for the determination, exercise or defence of legal claims;
- the data subject has objected to the processing.

The data subject shall be informed of the restriction operations actually implemented.

4.5 Right to data portability

The Data Controller, in compliance with the provisions of article 20 of the Regulation, guarantees, following an express request by the Data Subject, (a) the receipt by the Data Subject of personal data concerning him/herself in a structured, commonly used and machine-readable format; (b) the transmission of such data to another Data Controller without any impediment by the Data Controller to whom he/she has provided them and under the conditions provided for by the applicable law when their processing is based on the consent of the Data Subject or on the basis of a contract entered into with the Data Subject.

5. Privacy Management System

5.1 Risk Assessment, Gap Analysis, Remediation Plan and information flows

Snam carries out risk assessment activities periodically, or whenever there are organisational changes, in order to identify and manage the most significant risks in relation to the processing of personal data. If the conditions are met, a privacy impact assessment (DPIA) is also carried out in accordance with Article 35 of the Regulations.

Together with the risk assessment activities, Snam prepares a *gap analysis* of its Privacy Compliance Programme with respect to the reference best practices.

If the analysis shows that it is necessary to intervene by introducing the necessary changes to the business processes concerned for privacy-related aspects, Snam prepares and implements a remediation plan in order to make the Privacy Compliance Programme fully effective and in line with the new features introduced.

The monitoring and supervision of the above-mentioned activities is ensured by the presence of information flows to the Data Controller, including a specific declaration by each Delegated Data Processor on the compliance of the corporate activities carried out and involving aspects related to the rules on personal data processing. If the Delegated Data Processor identifies inconsistencies or breaches of privacy, he/she must refer the matter to the Legal Department in order to define and implement the necessary remedies.

5.2 Privacy Impact Assessment

At Snam, each processing operation, in any business area, must be configured in such a way as to provide, from the outset, the essential and functional guarantees for the protection of the rights of the data subjects. In compliance with the principles of *privacy by design* and *by default*, Snam adopts the security measures expressly provided for by law and other measures appropriate to its business context. Appropriate technical/organisational systems are therefore implemented to minimise processing and ensure the best outcome with respect to the actions of the *Privacy Compliance Programme*.

On the basis of the mapping of the processes emerging from the risk assessment and gap analysis activities and on the basis of the risk assessment related to each corporate process of reference as identified in the Register of Processes (as per paragraph 5.4 below), the Delegated Data Processor shall carry out a privacy impact assessment (DPIA) in accordance with the provisions of the Regulations and in line with the relevant best practices, whenever

the processing of personal data is likely to present a high risk to the rights and freedoms of natural persons.

5.3 Privacy policy

The Data Controller or the Delegated Data Processor must provide full information to the data subject from whom personal data are collected.

In particular, specific information must be released (by way of example) to:

- candidates at the information interview;
- employees at the time of recruitment (including non-permanent staff such as interns, project staff, secondments and management staff);
- suppliers/contractors during the preliminary assessment for qualification purposes;
- owners of property from which easement or ownership rights are acquired;
- shareholders;
- directors and statutory auditors;
- auditors;
- visitors, including in cases of video surveillance.

5.4 Processing Register

The keeping of a Data Processing Register is provided for in Article 30 of the Regulations, which considers it as a tool enabling more effective management of *data protection* within the organisation. This fulfils a number of purposes, including:

- keeping track of processing operations carried out within the individual organisation;
- constitute an operational working tool by means of which to survey in an orderly manner the databases and other relevant elements to ensure an effective «management cycle» of personal data;
- help to assess the inherent risk associated with each processing.

The Data Controller shall keep a register of the processing activities carried out under its responsibility.

This register contains the following information:

- the name and contact details of the Data Controller and the DPO;

- the purposes of processing;
- a description of the categories of data subjects and categories of personal data;
- the categories of recipients to whom the data have been or will be disclosed, including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of the third country or organisation and, for transfers pursuant to Article 49, par. 2 of the Regulation, documentation of appropriate safeguards;
- where possible, the deadlines for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 32, par. 1 of the Regulation.

The Register is periodically updated by the Legal function in agreement with the DT&T function which, for this purpose, must be promptly informed by the Data Processor in the event of new processing operations.

5.5 Security measures

Each Delegated Data Processor shall, in cooperation with the Legal Department and the DT&T and Global Security departments, identify suitable and preventive security measures in order to: (a) ensure a level of security appropriate to the risk of the processing, in order to ensure, on a permanent basis, the confidentiality, integrity, availability and resilience of the processing systems and services; (b) promptly restore the availability of and access to personal data in the event of an “*incident*”; (c) minimise the risks of destruction or loss, even accidental, of the data, of unauthorised access or of processing that is not allowed or does not comply with the purpose of the collection (see, also, Section 5.7).

The definition of precise and adequate security measures takes place after the risk assessment process on the processing of personal data by the Delegated Data Processor or Data Processor in cooperation with the Legal, DT&T and Global Security departments.

5.6 Personal data breaches

A *data breach* is a violation of the security standards adopted for the protection of personal data, which may result in the destruction, deletion, or alteration of personal data, the

loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed (e.g. data theft)³.

Pursuant to applicable legislation, Snam notifies events that represent a breach of security to the Supervisory Authority and to the Data Subject⁴. For notification to the Supervisory Authority, the Legal function coordinates the collection of all the necessary documentation and information.

Following a data breach, the Compliance Officer takes all necessary corrective actions in accordance with the security measures indicated in the preceding paragraph 5.5, assessing with the specialist support of the aforementioned functions the need and/or opportunity to increase the security measures in order to raise the general standards of data protection.

At Snam, the data breach procedure is governed by a specific regulatory instrument designed to identify the roles and responsibilities related to and involved in the process and aimed at ensuring compliance with legal obligations within the timeframe indicated in the Regulations.

5.7 Privacy by design and by default

The principle of Privacy by Design, introduced by the Data Protection Regulations, requires a proactive approach to personal data protection, which makes it necessary to provide for operating methods and security measures to safeguard the confidentiality, integrity and availability of personal data as they “enter” the organisation.

The Data Controller - taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, and the risks of varying likelihood and severity to the rights and freedoms of natural persons represented by the processing - both when determining the means of the

³ A data breach means a significant, but temporary, disruption of the operational continuity of an information system resulting in the compromise of even one of these elements:

- confidentiality breach or unauthorised or accidental disclosure of or access to personal data;
- availability breach, when there is a loss, inaccessibility, or destruction, again unauthorised or accidental, of personal data;
- integrity breach, when there is an unauthorised or accidental alteration of personal data.

⁴ Not all data breaches give rise to an obligation to notify the Supervisory Authority, and not all breaches notified must be communicated to the data subjects. The crucial element is the assessment of the estimated risk to the rights and freedoms of data subjects as a consequence of the personal data breach. If the risk is not probable, the Controller shall not notify the Supervisory Authority and obviously not even notify the data subjects. However, it will be required to keep track of the event (Art. 33.5 of the Regulations) and the risk analysis carried out in this respect, for future consultation and verification (principle of accountability).

processing at the time of processing itself, implement appropriate technical and organisational measures aimed at effectively implementing the principles of data protection and integrating the necessary safeguards into the processing in order to meet the requirements of the Regulation and to protect the rights of the Data Subjects.

The Data Controller puts in place appropriate technical and organisational measures to ensure that only the personal data necessary for each specific purpose are processed. In particular, these measures ensure that personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person.

In this context, Snam has adopted an integrated internal control and risk management system, and has implemented a personal data protection system aimed at optimising, as its own control tools in this area, further corporate control tools designed to guarantee adequate security measures in the field of personal data protection on an *ongoing basis*.

For each development/modification of the applications in use, the impact for privacy purposes is assessed, depending on the type of data processed by the application.

Furthermore, by default the Controller has, also, adopted:

- a data classification management system, which makes it possible to determine the types and relative criticality, in terms of confidentiality, of the information processed on the basis of the data contained therein;
- a programme of periodic technical audits; to identify any application or infrastructure vulnerabilities that may compromise the security of personal data;
- an integrated risk assessment system, on the basis of which to identify the exposure of personal data to risk and the consequent organisational, procedural and technological measures to be put in place to safeguard their security. The measures identified will feed into the list of security requirements that applications and supporting technology infrastructures must meet to protect the integrity and availability of personal data;
- a "Security Information and Event Management", through which log files are directed to a centralised analysis system that allows, on the basis of appropriate correlations, to identify anomalous activities potentially attributable to different types of vulnerability and cyber attack. Through correlation activities it is therefore possible both to activate preventive behaviour and to reconstruct the dynamics of an anomalous event (e.g. *data breach*) downstream of its occurrence;

- a device encryption system, Encrypting data within corporate devices such as smartphones and computers makes the data they contain accessible only to those who know the access key, while keeping them encrypted and therefore unreadable otherwise;
- a segregation system linked to roles and responsibilities with access limited to personal data strictly necessary for the performance of the tasks assigned.

6. Operational procedures for processing personal data

6.1 Documentation archiving

At Snam, documentation is archived in the form that has the least impact, both at organisational and environmental level, while at the same time taking into account the security measures to be adopted.

The archives of deeds and documents, including those in electronic format, containing personal data are subject to control and preservation for the time necessary for their processing.

For reasons of confidentiality and protection of personal data, in order to avoid any disclosure, access to the archives may only take place by the Delegated Data Processor or by another Officer in charge of processing if appointed. Access by other parties must be duly authorised.

With regard to appointments of Officers in charge of processing, the Delegated Data Processor shall keep, update and make available the list of Officers in charge of processing in his/her area of competence.

6.2 Data retention

Data shall be retained for a period not exceeding that which is strictly necessary for the purposes for which they were collected. Data retention times are determined taking into account, among others, the following criteria:

- purpose of use of personal data collected;
- pursuit of a legitimate interest and/or right of the data controller or a third party;
- legitimate interest and/or right of the data subject in relation to the activity for which the processing of personal data is required;
- type and/or extent of service/activity offered to the Data Subject and in relation to which personal data is processed.

The retention periods, defined on the basis of the criteria listed above, are set out in the Register of Processing and identified in each information note form.

6.3 Processing of personal data by means of video surveillance systems

For Snam, the purpose of video surveillance, where provided, is to protect people and property from possible attacks, theft, robbery, damage, acts of terrorism, subversion and vandalism, prevention of accidents in general and safety at work.

The use of a video surveillance system or installation, where a security risk has been identified, is limited to the protection of persons, property and assets of the company and, in particular:

- a) control of certain critical areas (e.g. National Gas Dispatching, Data Processing Centres, gas compression and/or storage plants, etc.), where there is an effective and proportionate need to prevent and repress offences;
- b) control of other areas (e.g. car parks, entrances), where there is a genuine and proportionate need to prevent and suppress offences;
- c) protection of the company's assets, including owned or rented property, also in order to avoid damage to regular and non-regular visitors to the structure (employees, consultants, visitors, suppliers, etc.).

Video-surveillance systems/plants, in compliance with the provisions of Article 4 of the Workers' Statute, may not be used to carry out controls on the work activities of employees of the Company or of other employers, whether public or private, even on a temporary basis.

The Global Security & Cyber Defence Head is the Delegated Data Processor for data processed through video surveillance systems for all plants installed within the Snam Group.

7. Roles and responsibilities

7.1 Personal data controller

The personal data controller at corporate level is identified as the legal entity that determines the purposes and means of personal data processing (Snam S.p.A. or each company in the group in relation to the ownership of the relationships to which the data relate).

7.1.1 Joint controllers

Joint controllers of personal data are identified where the purposes and means of processing are determined jointly by Snam and another company in the group. The joint controllers shall specifically define with

a specific deed their respective sphere of responsibility and tasks with particular regard to the exercise of the rights of the data subjects.

7.2 Privacy Compliance Officer

At Snam, this is the natural person within the company organisation who is responsible for independently fulfilling the obligations laid down in relation to the processing of personal data and exercising the rights and powers provided for by the Regulations for the Data Controller, as well as the power to identify within the company organisation the figures to whom specific delegated powers should be given.

In particular, the Compliance Officer, identified for each company of the group⁵, is vested with the widest powers and authorities to perform all the acts and fulfilments provided for by current legislation on the protection of personal data.

7.3 Data Protection Officer

The Data Protection Officer is a figure introduced by the Regulation to whom the tasks provided for in Article 39 of the Regulation are assigned⁶. The DPO, identified by the Head of Compliance, performs the tasks in coordination with the DT&T, Global Security & Cyber Defence and Organisation functions, also within the Cyber Security Committee.

Data subjects may contact the DPO for all matters relating to the processing of their personal data and the exercise of their rights under the Regulations, sending the request to: dataprotectionofficer@pec.snam.it.

The DPO reports periodically - in any event at least annually - on the activity carried out to the Compliance Officer of each company concerned.

⁵ The Compliance Officers at present are: for Snam S.p.A. the EVP Human Resources & Organization and for the subsidiaries their respective Managing Directors.

⁶ Article 39, par. 1 of the Regulations: *"The Data Protection Officer shall be responsible for at least the following tasks: (a) informing and advising the data controller or the processor as well as the employees carrying out the processing about the obligations arising from this Regulation as well as from other Union or Member State provisions relating to data protection; b) monitor compliance with this Regulation, with other Union or Member State provisions on data protection and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in processing operations and related monitoring activities; (c) to provide, where requested, an opinion on the data protection impact assessment and to monitor its implementation pursuant to Article 35; d) cooperate with the supervisory authority; (e) act as a contact point for the supervisory authority on matters related to the processing, including prior consultation referred to in Article 36, and carry out, where appropriate, consultations on any other matter"*. Although Snam is not one of the parties formally obliged to identify the DPO, it has decided to do so in line with best practice, including the recommendations of the Data Protection Authority and Art. 29 of the Working Party.

7.4 Data Processors

The Compliance Officer designates and assigns the relevant powers, also through delegated persons, to the (external) Data Processors pursuant to art. 28 of the Regulations and, within the company organisation, to the Officers in charge of Processing.

7.4.1 (External) data processor

The Data Processor within the meaning of art. 28 of the Regulations is the person who carries out a processing operation on behalf of the Controller, providing sufficient guarantees to implement all appropriate technical and organisational measures for the processing of personal data in such a way that the said processing meets the requirements of the Regulations and ensures the protection of the Data Subject.

The Data Processor processes the data in accordance with the instructions of the Controller and assumes responsibility for it.

The Data Processor must comply with all the obligations and duties provided for by the applicable law, such as by way of example but not limited to: the adoption of appropriate technical and organisational measures to ensure the security of processing.

The Data Processor has transparency obligations, so he must make available to the Controller all the information necessary to demonstrate compliance with the obligations imposed by Article 28 of the Regulation.

The person in charge is also obliged to ensure data security. Both the Data Controller and the Data Processor are required to implement technical and organisational measures taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, and the likelihood and severity of the risk to the rights and freedoms of natural persons.

Finally, the Data Processor must consent to and contribute to the review activities, including inspections (or audits), carried out by the Data Controller and must notify the Data Controller if it considers that an instruction it has received violates any of the relevant rules, must assist the Data Controller in fulfilling requests from data subjects.

If the conditions are met, the Data Processor is appointed within the framework of the relevant contractual relationship, by the attorney authorised to sign the contract, by means of a specific clause, provided for in the contractual standards defined by the Legal Department, which provides, *inter alia*, for the commitment of suppliers/contractors/subcontractors to comply with the criteria, purposes and methods of processing of personal data laid down by the

Regulations and by any instructions given by the Customer, as well as specific controls and supervision of the activities of the Data Processor.

It should also be taken into account that: a) in the event of framework agreements, relating to activities involving the processing of personal data, to which companies other than the company that signed the framework agreement may adhere (through application agreements), each company must independently appoint the Data Processor; b) if the activities covered by the contract involving the processing of personal data are subcontracted, the Data Processor must appoint the subcontractor as sub-processor, subject to authorisation by the Controller. It is understood that, in the event of authorisation by the Data Controller, the sub-processor shall be subject, by means of a contract or other legal deed, to the same data protection obligations as those contained in the deed appointing the Controller, providing in particular sufficient guarantees to put in place appropriate technical and organisational measures so that the processing meets the requirements of the Regulations. However, it is understood that, in the event of failure by the sub-processor to comply with its data protection obligations, the Processor retains full responsibility towards the Controller for compliance with such obligations.

The Data Processor may appoint sub-processors for specific processing activities on behalf of the Data Controller and with his/her prior authorisation.

7.4.2 (Internal) Delegated Data Processor

The Delegated Data Processor (internal Data Processor) is the person within the company organisation who holds the position suitable for functional competence to ensure and guarantee the maintenance of the control measures put in place to protect the rights of the data subjects and to implement, within the processes under his/her responsibility, all the appropriate technical and organisational measures for the processing of personal data.

The Delegated Data Processors shall comply with all the obligations and duties provided for by the applicable law, ensuring the adoption of suitable technical and organisational measures to guarantee the security of processing operations and their maintenance over time, also through a periodical reassessment of the degree of inherent risks related to the processes for which he/she is responsible.

The list of Officers in charge of processing can be found on the Intranet site, section "Summary Organisational Documents". This list must be kept up-to-date at the Organisation function, communicated to the DPO and made available in a timely manner, in case of

need, to the unit responsible to deal with third parties (e.g. following a request from the Data Subject).

The Organisation function shall submit to each Delegated Data Processor the letter of appointment, signed by the Compliance Officer, to be signed for acceptance.

7.4.3 Officer in charge of Processing

The Delegated Data Processor, if appointed, and within the limits of the specific processing activities delegated, shall appoint the Officer in Charge of Processing with specific instructions for carrying out the assignment, including the management and use of the databases to which they have access. The Officer in charge of Processing operates under the direct authority of the person who appointed him/her and may be the head of the organisational unit or may be any employee of the unit itself and belonging to the area of competence, who carries out the processing of personal data.

7.5 System Administrator

The System Administrator may be either internal or external to Snam. The Delegated Data Processor appoints the System Administrator, specifying the scope of operations and the application area. The latter is chosen from among employees who meet the following requirements:

- a) competence in IT based on experience, skills and professionalism, also with regard to IT security issues;
- b) compliance with legal provisions, including internal ones, on the processing of personal data.

By way of example but not limited to, System Administrators have the following responsibilities:

- making back-up copies (data backup and recovery operations);
- organisation of network flows;
- management of storage media;
- hardware maintenance;
- custody of credentials;
- management of authentication and authorisation systems.

The appointment of a System Administrator is made after assessing the experience, skills and reliability of the person appointed, who must

provide appropriate guarantees of full compliance with the applicable processing provisions, including the security profile.

The following persons may be identified as System Administrators:

- IT expertise, including in relation to security-related issues, e.g. in view of educational background, professional experience, etc.;
- compliance with legal and company regulations on the processing of personal data.

The System Administrator shall be designated individually by the relevant Delegated Data Processor in accordance with the above criteria, by means of a letter signed by him/her.

The System Administrator shall date and sign the document.

The signed letter, with an analytical list of the permitted areas of operation on the basis of the authorisation profile assigned, is sent to the HRO function, for filing in the employee's personal folder, and to the DT&T function for processing/updating the list containing the identification details of the natural persons appointed as System Administrators. This list must be kept up-to-date in the DT&T department and communicated to the DPO.

IT Systems must also be equipped with systems suitable for recording access (computer authentication) by System Administrators. The records (logs) must be complete, unalterable and it must be possible to verify their integrity. The logs must include time references and a description of the event that generated them and must be retained for a period of not less than six months.

The external party to whom system administration services are outsourced is appointed as Data Processor.

The contract also includes a standard clause governing the obligations of the outsourcer with regard, in particular, to the appointment of system administrators and the verification of their activities, as well as the keeping of an updated list containing the identification details of the natural persons appointed as System Administrators. This list shall always be made available and updated at the request of the Contract Manager.

In the case of existing contracts, the Contract Manager shall send the outsourcer, after informing the competent procurement function, a letter setting out the obligations to be observed in relation to System Administrators.

8. Operational tools

The forms and standards to be used in the privacy management system, prepared and updated by the Legal Department, are available on a special section of the corporate intranet, including:

- a) Standard Privacy contractual clause(s);
- b) Powers of the Compliance Officer;
- c) Letter template of appointment of Delegated Data Processors;
- d) Letter template of appointment of the System Administrator;
- e) Letter template of appointment of the Officer in charge of Processing;
- f) Information notes;
- g) Declarations of conformity of IT systems for the purposes of the Regulations;
- h) Template of notification to the Supervisory Authority in case of data breach;
- i) Model of communication to the data subject in the event of a data breach.

9. Training and communication

In order to ensure the correct and timely implementation of internal control systems with respect to the applicable legislation and related amendments on privacy, continuous updating is carried out at Snam for those data subjects involved in complying with the relevant regulations.

Professional privacy training is ensured by means of specific training courses which must be attended by employees appointed as Internal Data Processors, System Administrators or Parties processing the data. The content of the training courses varies for each of the figures listed above given the different powers and capacities recognised by the applicable legislation.

10. Responsibility for updating

The Legal function periodically reviews this Guideline and related operational tools to ensure their effectiveness over time and adherence to best practices.

All business units/positions involved in the activities described above are responsible, for the part under their responsibility, for detecting business occurrences that lead to the need for adaptation of this Guideline and for reporting them. The Legal function, in cooperation with the Organisation function, ensures the coordination of its updating activities.