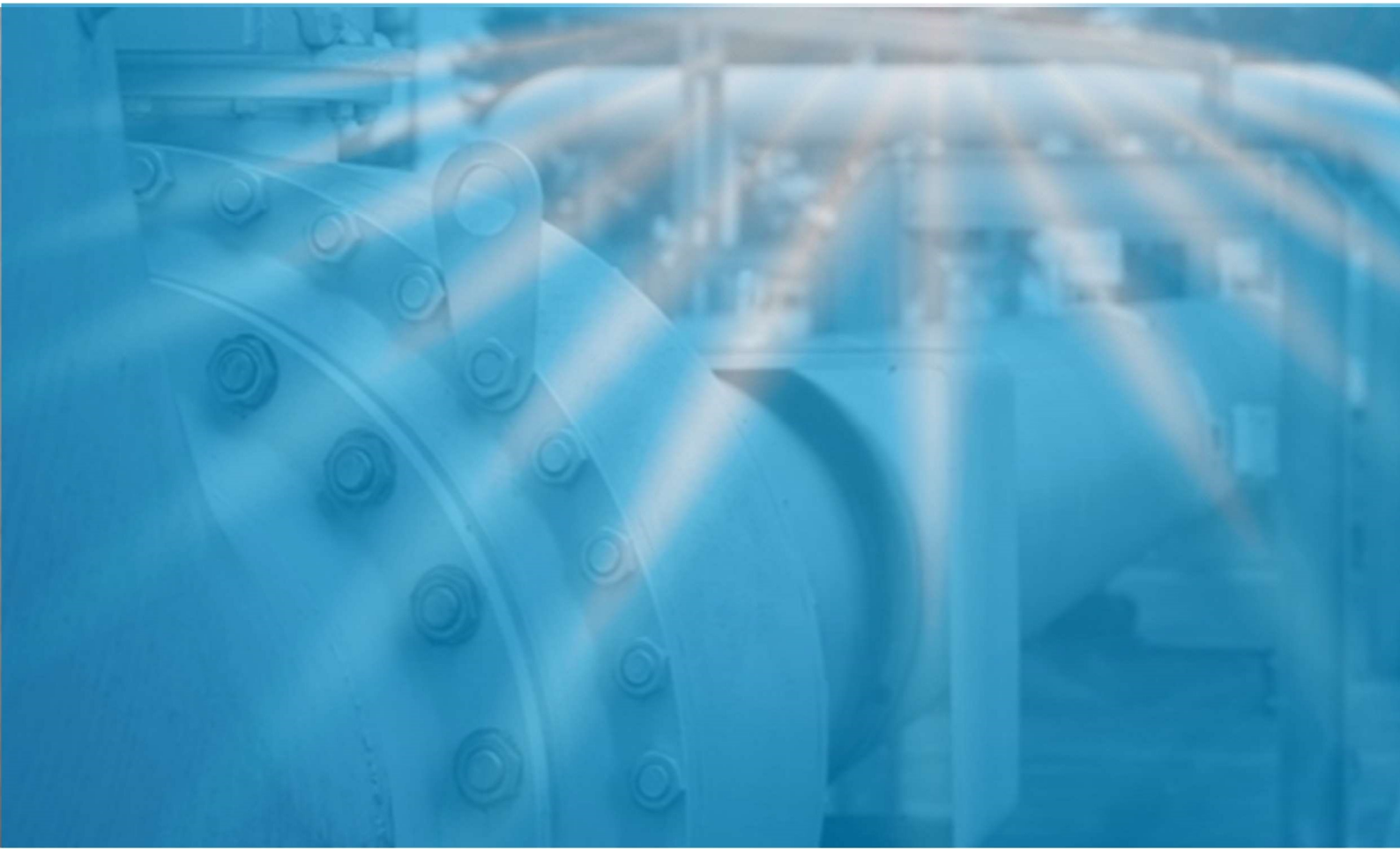
Compliance Standard

Data Breach Management



ITH-STC-077-R00
Issue date: 25/03/2019
Date effective: 25/03/2019

Written	SECUR
Verified	ICT HSEQ HRO ALESOC DPO
Approved	CEO
Elements of Compliance	**GDPR**[1]

Chronology of Reviews

- Rev. 00 (First issue)

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.

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

1 GDPR General Data Protection Regulation 679/2016

CONTENTS

1. Abstract

This standard on Data Protection activities applies to Italgas Group, pursuant to the scope of direction and coordination activities exercised by the former.

The standard aims to:

- provide information on the "Data Breach Management Process" the purpose of which is to ensure the governance and implementation of the process of managing personal data violations in order to notify the control authority of any breaches;
- define all the aspects necessary to tackle any crisis situation, providing the organisational units involved in launching a "Data Breach Plan" with a tool and guiding them in the correct adoption of the solutions proposed;
- identify the roles and responsibilities of the various subjects involved who participate in the application of this procedure.

According to the provisions of the WP250 "Guidelines on Personal data breach notification under Regulation 2016/679," potential Data Breach events can be divided into three macro categories:

- "**Confidentiality breach**": in the event of the unauthorised or accidental disclosure or unauthorised access to personal data;
- "**Availability breach**": in the event of the accidental or unauthorised loss of access to data or the destruction of personal data;
- "**Integrity breach**": in the case of the unauthorised or accidental alteration of personal data.

By way of example, but not limited to such, some types of personal data breaches are described below:

- **destruction of computer data or paper documents** understood as the irreversible unavailability of data with its recovery being ascertained as impossible, caused by logical elimination (e.g. incorrect deletion of data during a manual or automated or physical operation, damage to computer storage devices, fire/flooding of premises where contracts and other customer documents are filed);
- **loss of data**, resulting from the loss/theft of electronic storage media (e.g. Laptop, HD, Memory Card) or contractual documentation or other paper documents (originals or copies);
- **unauthorised access or intrusion to computer systems** understood as exploitation of the vulnerabilities of the internal systems and communication networks or through compromised or the improper detection of authentication credentials (e.g. user ID and password) for access to the systems;
- **unauthorised modification of data**, deriving for example from the incorrect execution of interventions on computer systems or from human interventions;
- **disclosure of data and documents to unauthorised third parties**, including unidentified ones, resulting for example from the supply of information, including minutes, to people other than the entitled person (in the absence of a formal mandate from the latter), the sending of invoices or other documents of contractual, executive value or the incorrect management of electronic storage devices.

2. Departments Involved

Department Mentioned in this document	Organisational Unit
Security Department	Security (SECUR)
Legal Department	Legal & Corporate Affairs and Compliance (ALESOC)
External Communication Department	External Relations and Communication (RELECOM)
Human Resources Department	Administration and HR Services (AMMSER)
ICT Department	Information and Communication Technologies (ICT)
Institutional Relations and Regulatory Affairs Department	Institutional Relations and Regulatory Affairs (REISAR)

3. Compliance principles

3.1 Roles and Responsibilities

The following table describes the roles and responsibilities covered in this operating procedure and set out in the subsequent check lists.

Operational Roles	Description
Data Protection Officer (DPO)	This figure monitors the company's compliance with the provisions of the GDPR and is the key point of contact with the Authority and the data subjects.
Privacy Incident Resolution Team (PIRT)	This team is composed of: • Head of ALESOC unit; • Head of ICT unit; • Head of FINSE unit; • Head of SECUR unit; • Head of REISAR; • Head of RELECOM; • Data Protection Officer (DPO); • Compliance Manager, and the Data Managers involved in the "Privacy Incident" who determine an adequate plan of action to resolve the "Privacy Incident" detected.
Data Manager	Natural person included in the Company organisation and in charge of performing certain operations concerning the monitoring and coordination of Processing carried out on Personal Data.
Incident Reporter	Employees of the Italgas Group (users) who report a potential Privacy Incident. Moreover, the reports can be made by external staff, customers and suppliers.
Compliance Manager	Manager that has the necessary corporate powers and adopts organisational measures to ensure the evaluation, definition and coordination of company initiatives and is responsible for fulfilling and exercising the rights and powers assigned to the Data Controller.

Support roles	Description
Data Protection Team	This Team is made up of representatives of the SECUR, ICT, HRO and ALESOC Units and supports managers in Privacy-related matters.
Line Reference Person	Natural person who acts as a focal point for all matters pertaining to Data Protection within their Organisational Structure/Company. The processing reference persons support the Data Processor. They ensure oversight of the processing operations in the day-to-day activities.
System administrators	Person In Charge of managing the IT systems used to process the personal data.

They can be called upon to support the Data Breach Management Process of all other Group departments in order to ensure the correct performance of the operating activities.

3.2 Data Breach Process

The aim of the Data Breach Management Process is to:

- handle reports of any Data Breach events and confirm the occurrence of a Privacy Incident;
- assess the seriousness of the breach, on the basis of the methodology defined and reported in an annex to this document (Preliminary Assessment) in order to estimate the potential risk for the rights and freedoms of the natural persons. This assessment is necessary to establish whether or not to notify the Data Protection Authority and if necessary the data subjects involved.

The breach notification must be sent without undue delay by and no later than 72 hours after it came to light, unless the personal data breach is unlikely to present a risk to the rights and freedoms of the natural persons. In accordance with Article 33, paragraph 1, the Italgas Group is not required to notify the Authority if, after the analyses conducted, the risk is not considered high. Nonetheless, a documentary trace must be kept of it in the Data Breach Register.

If the notification to the control Authority is not made within 72 hours, it must be accompanied by the reasons for the delay. Moreover, in situations where the personal data breach may generate a high risk for the rights and freedoms of the natural persons, the companies of the Italgas Group (as Data Controllers) must inform the data subject without undue delay.

In situations where the Italgas Group has assigned the services to a supplier, this latter must promptly inform the Group of any Data Breach cases in accordance with the provisions of articles 33 and 34 of the GDPR.

In order to comply with the provisions of the GDPR, all personal data breaches that occur within the Italgas Group must be managed in line with the provisions, in the following phases:

- **Phase 1 - Identification**: identify, by means of a preliminary assessment, if the reports received can be defined as a Privacy Incident;
- **Phase 2 - Assessment:** assess the importance of the Privacy Incident by estimating the potential risk associated with the rights and freedoms of the natural persons. This activity is essential to establish whether or not to notify the Data Breach to the Data Protection Authority and if necessary the data subjects involved;
- **Phase 3 - Response:** formalise the report and notify the Data Protection Authority that a Data Breach has occurred using a specific form and, if necessary, inform the data subject;
- **Phase 4 - Resolution:** implement the corrective action plan with the aim of mitigating the risk identified and arrange for prompt action to be taken in order to contain and manage the Privacy Incident identified as well as possible;
- **Phase 5 - Post Incident Review:** carry out an ex-post examination of how the Privacy Incident was handled so that an incident closure report can be prepared.
  This report must be sent to the Data Managers involved and must include:
  - the main causes of the event;
  - the actions taken to overcome the critical issues that emerged;
  - any opportunities to improve the company processes.

A description of the Data Breach process is set out below in the form of a flow diagram.

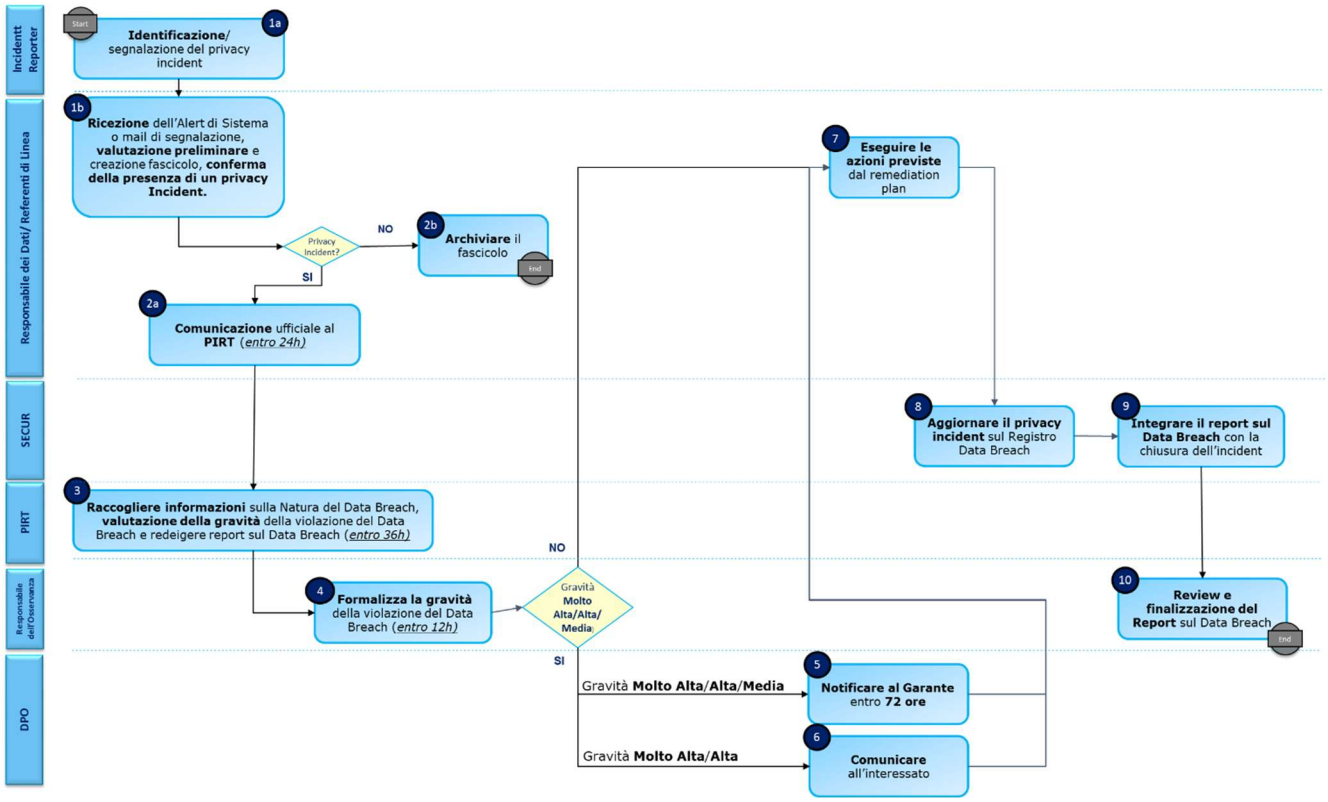


Figure 1: Data Breach process

Legenda

Legenda	Descrizione
	Step del processo
	Verifica

3.3 Operating Procedures for the Management of Data Breach

This section provides a detailed illustration of the operating instructions to be followed if a potential Privacy Incident is identified. In particular, the following information is shown for each phase:

- **Checklist/Tables** that describe the actions that must be taken and the Owner of the activities in the "Role/Person In Charge", "Activities", "Description of the activity";
- **Support material** represented by all external documents referred to in the checklists/tables in the "Tools" column.

3.3.1 Phase 1: Identification

The reports received by email or system alert from employees/external staff/customers or suppliers must be undergo a preliminary assessment, the aim of which is to confirm whether or not a Privacy Incident has occurred.

3 different communication flows have been identified within the Italgas Group depending on the type of Privacy Incident. In particular:

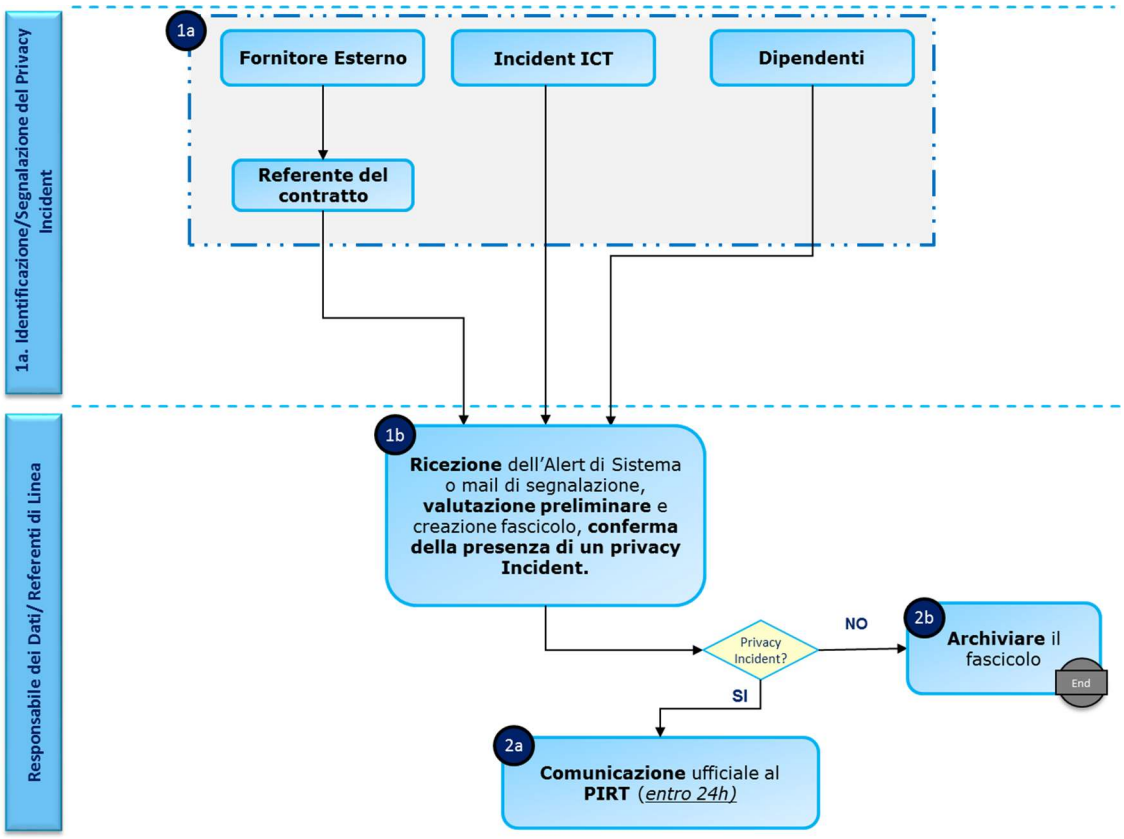


Figure 2: Privacy Incident reporting process

ID	Role	Activity	Activity Description
1a	Incident Reporter (employees/ external staff/ suppliers)	Identification and reporting of the Privacy Incident	Identifies a potential Privacy Incident by sending a report in the following cases: • If the Incident Reporter is an external supplier, the latter shall send the template prepared (annex 4.4) to the contract reference person who shall send this report to the Data Managers of reference for the processing carried out; • If the Incident Reporter is an employee, the latter must inform the Data Manager of the processing carried out.
1b	Data Manager	Receipt of the System Alert or reporting e-mail, preliminary assessment, file creation and confirmation of the occurrence of a Privacy Incident	Receives the report, makes a preliminary assessment by obtaining all the information on the event that occurred and creates a file in order to check, potentially with the support of the DPO and head of ICT, whether a Data Breach has occurred. If a Data Breach is confirmed, **"activity 2a."** shall be carried out. Alternatively, when the event is NOT considered a Data Breach, **"activity 2b."** shall be carried out.
2a	Data Manager	Summoning of the PIRT	Once a Data Breach has been confirmed, the Data Manager sends an official communication to the PIRT and summons this figure so that the necessary analysis can be carried out, and to i) assess whether to ask the Incident Reporter for further clarification or information; ii) confirm, or not, the preliminary analysis received on the existence of a Data Breach; iii) start activities to determine whether the breach is such that it presents a risk to the rights and freedoms of the natural persons, and the actions necessary to remedy it or mitigate the risks.

ID	Role	Activity	Activity Description
			This activity must be carried out within 24 hours after confirmation that a Data Breach has occurred.
2b	Data Manager	Archive the file	Archives the file when the event is NOT considered a Data Breach or when there is no knowledge or belief that the collection, access, alteration, loss and/or exposure of personal data has occurred in an improper or unauthorised manner, documenting the events that occurred – including the relative circumstances, consequences and measures adopted – in the Data Breach Register, which contains the identification and description of personal data breaches. In situations where the event is not considered a Data Breach, it will be handled like other security incidents as defined in the Group policy.

3.3.2 Phase II: Assessment

According to the provisions of Regulation EU 2016/679 art. 33 *"The controller shall document **any** personal data **breaches**, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."*

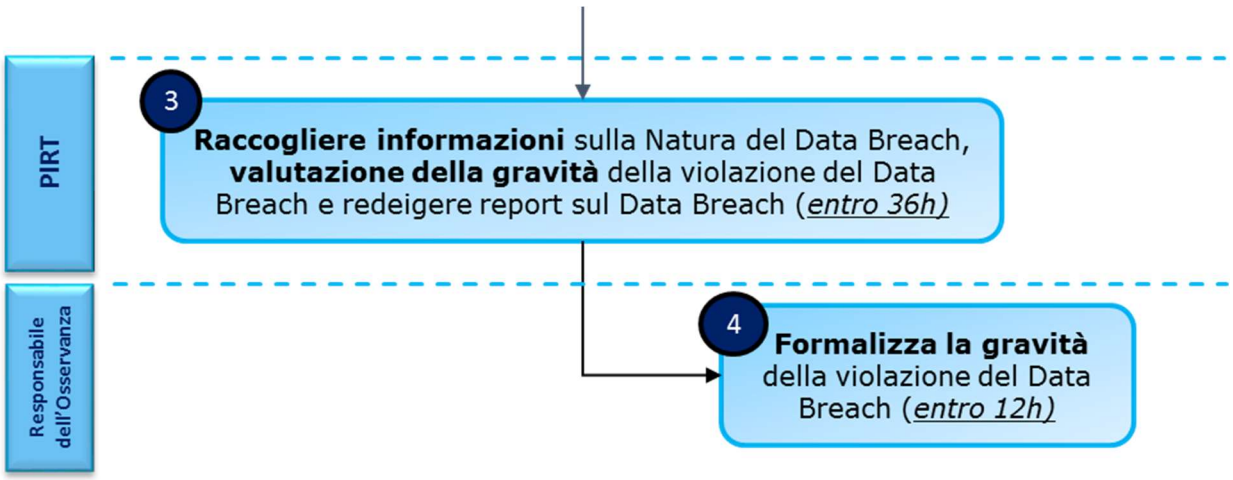


Figure 3: process of collecting information, assessment and formalisation

The following table describes the activities pertaining to the **assessment phase:**

ID	Role	Activity	Activity Description	Instruments
3	PIRT	Collection of information on the nature of the Data Breach	Collects additional information on the nature of the Data Breach and enters it into the Data Breach Register in order to classify the nature of the data breached and to keep track of the breach. In particular, this figure collects the following information on the event that occurred:	"Draft" Data Breach Register

ID	Role	Activity	Activity Description	Instruments
			• Type of personal data processed; • Volumes of data processed; • Persistence of the personal data in the system; • Completeness of the personal data processed; • Intelligibility of the data processed; • Number of users authorised to access the data; • Positioning on the network of the system that processes the data; • Security measures in place to mitigate the risk; • Time taken and procedures put in place for the final resolution of the event/incident.	
3	PIRT	Assess the severity of the Data Breach	Using the "Methodology of the assessment of severity of personal data breaches," structured on the basis of the ENISA guidelines[1] (see the document contained in Annex I,) the PIRT assesses the "magnitude" of the risk in order to estimate the potential risk to the rights and freedoms of the natural persons (in terms of financial and non-financial damage). This assessment is essential to understand whether or not to proceed with the notification to the Data Protection Authority and/or the data subjects involved.	Methodology of the assessment of severity of personal data breaches
3	PIRT	Report Data Breach	The PIRT prepares the report indicating the information required by article 33, paragraph 3, of the GDPR, and in particular: • A description of the breach, the categories and the number of data subjects involved; • A description of the likely consequences, indicating the degree of probability of the Data Breach presenting a risk for the rights and freedoms of the natural persons; • A description of the immediate measures to be adopted or those it is proposed be adopted; • A preliminary assessment of the risk based on the WP29 criteria of October 2017 [2] **These activities must be carried out within 36 hours after approval of the preliminary assessment.**	Report on the Data Breach containing the Remediation Plan (reference to the *Annexed Data Breach Report Template*)

1 European Network and Information Security Agency

2 The preliminary assessment of the risk must contain: the type of breach, the nature and volume of the data, the ease of identifying the data subjects, the severity of the consequences for the data subjects, the particular characteristics of the data subjects, the number of data subjects affected, the particular characteristics of the data controller.

ID	Role	Activity	Activity Description	Instruments
4	Compliance Manager	Formalisation of the severity of the Data Breach	Formalises the assessment of the severity of the Data Breach by i) confirming the report, approving the sending of a notification to the Authority and, if applicable, the communication of the breach to the data subjects; or ii) not confirming the report, indicating the reasons to be documented in the specific register; in any case iii) further clarifications and supplementations may be requested where necessary. It is specified that the validated assessment is reported in the final version of the Data Breach Register. **This activity must be carried out within 12 hours after receipt of the report made by the PIRT**	Data Breach Register

3.3.3 Phase III: Answer

In line with the provisions of art. 33 paragraph 3 of the GDPR, **at the end of the assessment and classification of the Data Breach** the following activities must be carried out:

- **Notification to the Authority:** the Data Protection Team, with the support of the DPO, prepares a report setting out the information required under art. 33 paragraph 3 of the GDPR. The PIRT, with the support of the DPO, prepares a report setting out the information required under art. 33 paragraph 3 of the GDPR. Once the report is complete, the DPO must fill in the specific reporting form prepared by the Data Protection Authority which the DPO will then send to the Authority within 72 hours (https://www.garanteprivacy.it/documents/10160/0/Allegato+1+Modello+segnalazione+data+breach+PA.pdf).
- **Notification to the data subject**: the DPO has the duty of informing the data subject that their personal data has been breached using simple and clear language and describing the nature of the breach, providing at least the information and measures referred to in art. 33 paragraph 3 of the GDPR.

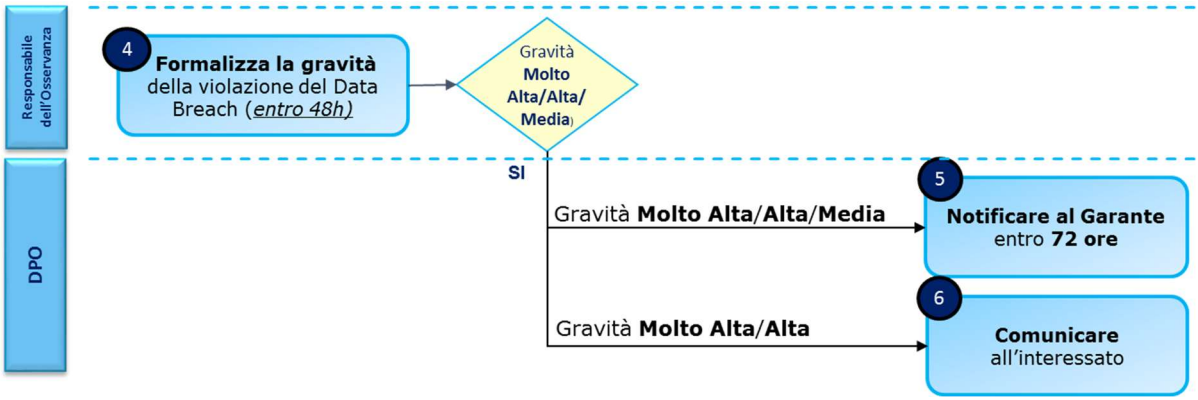


Figure 4: process of notifying the Authority and the Data Subject

The following table describes the activities pertaining to the **response phase:**

ID	Role/Person in Charge	Activity	Activity Description	Instruments
5	DPO	Inform the Data Protection Authority within 72 hours **(if the severity is Very High / High / Average)**	Fills in the specific Data Breach reporting form available on the institutional website of the Data Protection Authority (in cases of average, high and very high risk). The Data Breach notification must include at least the following information: • the nature of the personal data breach including, where possible, the categories and approximate number of people affected and the types and approximate number of personal data records in question; • the name and contact details of the data protection officer and any points of contact who can provide information; • the likely consequences of the personal data breach; • the measures adopted or proposed that the Data Controller can use to tackle the personal data breach, including any measure to mitigate the possible negative effects. If and to the extent that it is not possible to provide the information at the same time, the information may be provided at later stages without undue delay.	Reporting form
6	DPO	Inform the data subject **(if the severity is Very High or High)**	Informs the data subject by email or registered letter (in cases where the risk is high or very high for the rights and freedoms of the data subject), having checked the actual need for the communication (see next paragraph) In particular: - the name and contact details of the DPO or another point of contact from whom to obtain more information; - the likely consequences of the personal data breach; - the measures adopted or that it is proposed be adopted by the data controller to remedy the personal data breach and also, if applicable, to mitigate the possible negative effects.	E-mail with read receipt

With reference to the notification to the data subject, in accordance with the provisions of Regulation EU 2016/679 and the WP250 Guidelines on Personal Data Breach notification under Regulation 2016/679, such notification **is not required** in the following cases:

- the data controller has put in place adequate technical and organisational protection measures and these measures were applied to the personal data that has been breached, in particular those designed to make the personal data incomprehensible to anyone who is not authorised to access it, such as encryption;

- if the data controller adopted measures subsequent to the breach that guarantee a reduction of the risk for the rights and freedoms of the data subjects;
- if the notification to the data subject involves disproportionate efforts it must be made through a public disclosure or a similar measure through which the data subjects are informed in a just as effective way.

3.3.4 Phase IV: Resolution

According to the provisions of Regulation EU 2016/679 art. 33, the Data Controller must implement adequate measures to remedy the personal data breach and also to mitigate the possible negative effects after the Assessment of the severity of the personal data breaches and any notification to the Data Protection Authority and/or the data subjects.

Specifically, the "Remediation Plan" must contain:

- the organisational and technological actions that will be undertaken to respond to the breach in order to mitigate the negative effects and avoid a recurrence of the same crisis situation;
- the roles and responsibilities of the person appointed to implement the remediation actions;
- a Gantt chart to identify the timing and costs of the remediation actions.

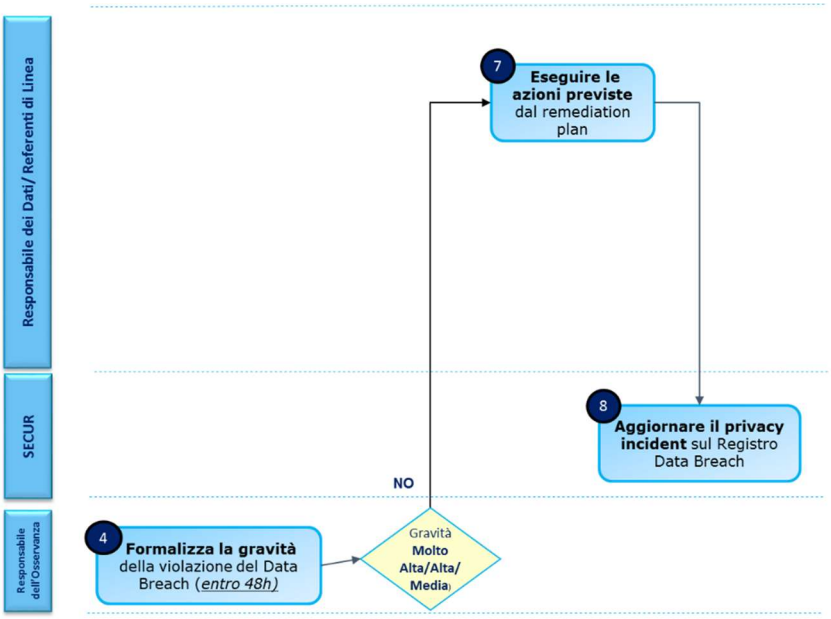


Figure 5: resolution process

ID	Role/Person in Charge	Activity	Activity Description	Instruments
7	Data Manager	Carries out the actions included in the Remediation Plan	Carries out the corrective actions plan which contains the actions to be taken to resolve the critical issues linked to the Incident detected.	Data Breach Report containing the Remediation Plan (annexed *Data Breach Report Template*)

ID	Role/Person in Charge	Activity	Activity Description	Instruments
8	SECUR Unit	Update the Data Breach Register	Once the corrective actions are completed, it updates the Data Breach Register with a full description of the event and the mitigation actions in order to keep track of what happened in the system and to be able to reconstruct the event if need be.	Data Breach Register (annex *Data Breach Register*)

3.3.5 Phase V: Post Incident Review

Once the Data Breach has been resolved, an ex-post examination is carried out on how the Data Breach was handled so that an incident closure report can be prepared.

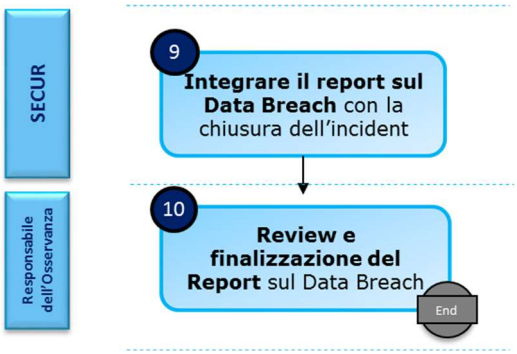


Figure 6: Post Incident review process

The following table summarises the activities of the Post Incident review phase:

ID	Role/Person in Charge	Activity	Activity Description	Instruments
9	SECUR Unit	Supplement the Data Breach report with the incident closure	Supplement the Data Breach summary report with a full description of the Incident, the root causes, the lessons learned and the improvement opportunities.	Data Breach Incident Report (annex *Data Breach Incident Template*)
10	Compliance Manager	Review and finalisation of the Data Breach Report	Send the report prepared to the Heads of the company Departments involved in the breach. The report contains: • full description of the event • mitigation actions • outcome and closure of the Incident The same is submitted to the meetings of the BoD, SB and BoSA.	Data Breach Incident Report (annex *Data Breach Incident Template*)

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.

5. LIST OF ANNEXES

Annex		Responsible for Updates
1	Support file Data Breach Management	SECUR