Compliance Standard

Data Breach Management

Document code: ITH-STC-077-R01

Issue date: 27/03/2024
Macro-Process: Compliance
Process: Data protection compliance
Subprocess: Data breach management

Written	SECUR					
Verified	IGLEGAL	REISAR	CYBSEC (BLU)	ORG&HROP	COMPLA	QUAL
	RELESOST	DPO				
Approved	AD					
Elements of Compliance	GDPR[1]					

Version History

- Rev. 01 – Main changes:
  - Introduced references to Guidelines adopted by the European Data Protection Board (EDPB) on 14 December 2021;
  - Improved accountability by introducing Phase II A to resolve and limit the effects of data breaches and specify the roles and responsibilities of the Compliance, Data and Contract Managers for the data breach management process;
  - Implementation of organisational changes.
- Rev. 00 (25/03/2019)

The company intranet is the official source of the documents in force. If you are using printed documents, you should always check that they are up to date with the original in force available on the company intranet.

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

[1] GDPR General Data Protection Regulation 2016/679

CONTENTS

1 ABSTRACT

This standard on Data Protection activities falls within the framework of the direction and coordination activities exercised by the Parent Company Italgas S.p.A.
The document is addressed to all Italgas Group Companies, personal Data Controllers and Processors individually and independently bound to comply with the requirements imposed by the applicable rules and regulations on personal data protection, and in particular on personal data breaches, and to the Departments and/or individuals in them who play a part in the breach management process.

A "*personal data breach*" is defined as "a security breach that accidentally or unlawfully results in the destruction, loss, modification, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed".

Data controllers and processors are bound by a series of obligations to ensure that incidents are rapidly investigated, to manage the potential effects of such incidents on data subjects and to ensure transparency to the Supervisory Authority and the said data subjects.

Specifically the Data Controller is bound to notify the Supervisory Authority of breaches without undue delay, where possible within 72 hours of it becoming known, except in cases where the breach is unlikely to present a risk to the rights and freedoms of the data subjects.
In cases of probable high risk, the breach must also be communicated to the data subjects.
This obligation implies the need for data managers to promptly report all incidents that may constitute personal data breaches to the Data Controllers, since each data breach constitutes a specific security incident[2].

It follows from the above, that technical and organisational measures must be taken to be able to quickly and effectively detect, assess and manage cases of potential breach.
The standard therefore aims to address the need to ensure, within the required time frame and in the required manner, the detection, assessment and notification, where necessary, of personal data breaches coming to the knowledge of Group companies acting as Data Controllers, by:

- defining a process that specifies the activities, roles, and responsibilities needed to effectively coordinate the phases of managing personal data breaches;
- defining instruments to guide the organisational units involved in the "Data Breach Management" process.

[2] as regards security incidents, please see the compliance standard ITH-STC-057 "Business continuity and emergency and crisis management"

2 DEPARTMENTS INVOLVED

Department Mentioned in this document	Organisational Unit
Security Department	Group Security (SECUR)

The "Privacy Incident Resolution Team" (PIRT) has been set up to handle the subsequent assessment phases of specific cases and consists of the:

- Privacy Compliance Manager of the Company involved in the «Privacy Incident»
- Data Managers involved in the «Privacy Incident»
- Head of the General Coounsel Unit (IGLEGAL);
- Head of the HR Regulated Business Unit (HR-REG);
- Head of the HR Non-Regulated Business Unit (HR-NR);
- Head of the Group Security & Real Estate Unit (SECUR);
- Head of Institutional Relations and Regulatory Affairs. (REISAR);
- Head of External Relations and Sustainability (RELESOST);
- Head of the Cybersecurity (CYBSEC) Unit of Bludigit S.p.A.;
- Data Protection Officer (DPO);

The PIRT decides how to manage the "Privacy Incident", assesses the risks to the data subjects deriving from the breach that has occurred, and defines an appropriate plan of action to resolve it.
PIRT meetings may also be held remotely via audio/video connection.

The Privacy Compliance Manager may invite representatives of other departments to the PIRT meeting, as he/she deems appropriate, especially in the event of absence/unavailability of one or more members of the PIRT.

The following parties are also involved in a supporting role:

- Data Protection Team
- Line Reference Persons
- System administrators

Consistently with the Data Protection Organisational Model, which defines the roles and responsibilities as set out in the "Data Protection"[3] Compliance Standard, assigned in accordance with the methods defined therein, the roles and responsibilities of the main parties involved in the Data Breach Management process are defined as follows:

- the **Privacy Compliance Manager** formalises the severity of privacy incidents, arranges for the notification to be sent to the Italian Data Protection Authority and performs a post incident review, to assess its management;
- the **Data Manager** must notify the PIRT of the possible presence of a privacy incident, carry out a preliminary assessment and take appropriate remedial action accordingly;
- the **Contract Manager**, in cases where the incident reporter is an external provider, must ask it to compile the dedicated template and forward it to the Data Manager.

Any other Group department may be called on to support the Data Breach Management Process to ensure the correct performance of operations.

3 COMPLIANCE PRINCIPLES

3.1 Aim and general requirements

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;

[3] ITH-STC-071 "Data Protection" Compliance Standard

- assess the seriousness of the breach, using the methodology defined and described in the annex to this document (*Annex 1 – Severity Assessment Method*) so as to estimate the potential risk to the rights and freedoms of natural persons. This assessment is necessary to establish whether or not to notify the Data Protection Authority and if necessary the data subjects involved.
- ensure that each Data Controller notifies the breach(es) to the Supervisory Authority, where necessary, and to the data subjects within the specified timeframe.

Notification of the breach to the Supervisory Authority must be made without undue delay and, where possible, within 72 hours of it coming to his/her knowledge, i.e. from when the Data Manager ascertains the existence of a "Privacy Incident", i.e. a personal data breach likely to present a risk to the rights and freedoms of natural persons. If the personal data breach is likely to present a high risk to the rights and freedoms of natural persons, the Data Controller is bound to also notify the data subjects of the breach, without undue delay[4].
Pursuant to Article 33, subsection 1 of the GDPR, Italgas Group companies are not required to notify the Authority if, after analysis, it appears that the personal data breach is unlikely to present a risk to the rights and freedoms of natural persons. Nonetheless, a documentary trace must be kept of it in the Data Breach Register.
In the case of more complex breaches, in order to fully establish the nature of the breach, the Data Controller may carry out notification in phases[5]. He/She makes a preliminary notification to the Authority within 72 hours, containing the information gathered up to such time on the Privacy Incident and an indication of the reasons for the delay, in accordance with Article 33, subsection 1, subsequently making a second notification after 72 hours, with additional information. 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 in any case inform the data subject without undue delay.
If the Italgas Group has entrusted services to a provider, the latter must promptly report any abnormal event to an internal contact person of the organisation, as indicated in the "Business Continuity and emergency and crisis management"[6] compliance standard; this internal contact person is the Contract Manager.
A specific clause in this regard must be included in the contractual agreements with the provider pursuant to Article 28 GDPR so that the obligation of the Data Controller to report any personal data breaches is guaranteed, as required by Article 33 GDPR.

3.2 Classification and examples of personal data breaches

A "*data breach*" is defined as "a security breach that accidentally or unlawfully results in the destruction, loss, modification, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed"[7].

According to the provisions of WP250 "Guidelines on personal data breach notification pursuant to Regulation (EU) 2016/679", possible Data Breach events ("Privacy Incidents") 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:
- **accidental 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 documents are filed);
- **loss of data**, resulting from the loss/theft of electronic storage media (e.g. Laptop, Hard Disk, Memory Card) or contractual documentation or other paper documents (originals or copies);

[4] The main purpose of notifying the data subjects is to provide them with specific information on the measures they can take to protect themselves from any adverse consequences of the breach. See GDPR, recital 86.
[5] WP250rev.01 "Guidelines on Personal Data Breach Notification Under Regulation"; GDPR, Article 33, para. 4
[6] ITH-STC-057-R01 "Business Continuity and Emergency and Crisis Management Compliance Standard"
[7] GDPR, Article 4, para. 12

- **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 parties.

Supplementing the WP250 Guidelines are further Guidelines reflecting the common experiences of European Data Protection Authorities since the GDPR became applicable, including Guidelines 01/2021 "Examples regarding Personal Data Breach Notification", adopted by the European Data Protection Board (EDPB) on 14 December 2021, version 2.0. The purpose of this document is to help data controllers decide how to manage data breaches and what factors to consider when assessing the risk.

3.3 Operating methods for managing breaches

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 documents referred to in the checklists/tables in the "Tools" column.

The process follows the standard phases described below. It should be emphasised that the compliance requirements imposed by applicable legislation weigh differently on the Group companies according to whether they are individually data controllers or data processors. In the first case, the notification obligation weighs on each controller company; in the latter case, there is no notification obligation, but only the requirement to promptly notify the controllers.

- **Phase I - Identification**: identify, by means of a preliminary assessment, if the reports received can be defined as a Privacy Incident;
- **Phase II A – Resolution and limitation of effects:** 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 II B - 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 III – Notification:** formalise the report and if appropriate communicate it to the Group companies which are Data Controllers. If necessary, notify the Italian Data Protection Authority of the Data Breach via the appropriate online service and, where applicable, notify the data subject;
- **Phase IV - 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.

The Data Breach management process is shown below in the form of a flow chart.

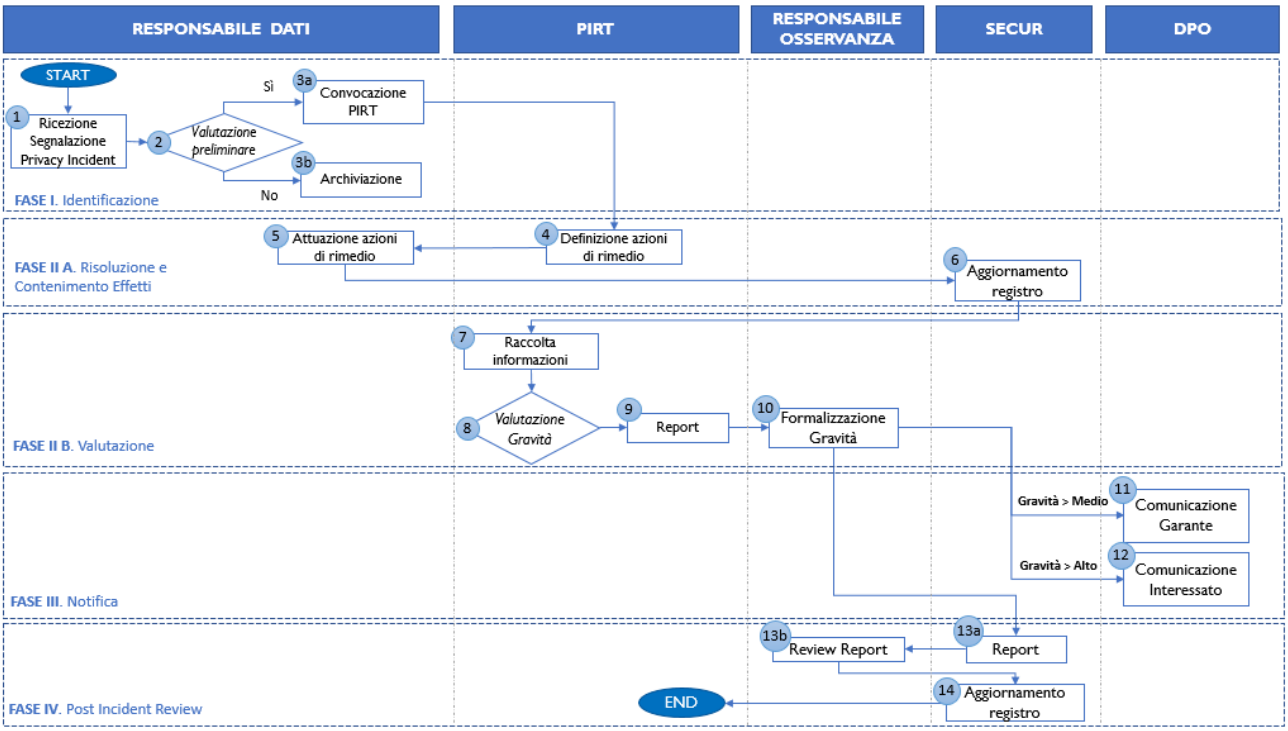

Figure 1: Data Breach management process

3.3.1 Phase I: Identification

The occurrence of an anomalous situation may emerge from reports from various sources:

- from **IT Departments**, as part of their security monitoring activities: these are situations of loss of integrity, availability, confidentiality of personal data, which may therefore have had a potential impact on the persons to whom the data refer;
- from **an external provider** or a Group Company, appointed as data processors. In these cases, the report is made by filling in a dedicated form attached to this procedure, complying with the timeframes and procedures defined in the deed of appointment pursuant to Article 28;
- from an **employee:** for example, the theft or loss of a mobile device (e.g. USB key, hard disk, mobile phone, tablet or laptop) containing personal data is reported;
- from other **external sources** such as the **Supervisory Authority** the **data subjects themselves**, the **media** or **other external channels**.

All reports of possible personal data breaches, received by e-mail or system alerts from employees/external collaborators/customers or providers, must be forwarded to the Data Manager responsible for the data processing carried out.
The Data Manager carries out a preliminary assessment, the aim of which is to confirm the Privacy Incident or not.

Privacy-related reports are forwarded by the Data Manager to the PIRT and are recorded by SECUR in the Data Breach Register[8].

Employees are required to report possible personal data breaches to the Data Processors of the processing performed. Instructions in contracts with providers include the obligation to report possible personal data breaches to the Data Controller by contacting the Contract Manager. Lastly, data subjects may contact the DPO at the e-mail address provided in all the privacy policies.

[8] Regardless of whether or not a breach must be reported to the Supervisory Authority, the Data Controller must keep records of all breaches. He/she is required to record the details of the breach, including the causes, the facts, and the personal data affected.

The following table describes the activities pertaining to the identification phase:

ID	Role	Assets	Activity Description	Instruments
1	Incident Reporter (employees/ external staff/ providers/other sources)	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 provider (Data Processor), the Contract Manager asks him/her to compile the dedicated template (in Annex 1) and immediately forwards it to the relevant Data Manager; • If the Incident Reporter is an employee, the latter must inform the Data Manager of the processing carried out; • If the report is made through another channel by an external party (e.g. data subject, media, etc.), it must be promptly forwarded to the relevant Data Manager. If the Data Manager is absent/unavailable, the communication must be addressed to the Privacy Compliance Manager.	Template for Data Breach Communication from the Data Processor (Annex I – *Communication Template)*
2	Data Manager	Receipt of the System Alert/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 whether a data breach has occurred. May request the support of the DPO and the IT Compliance and Cybersecurity Departments. If the presence of a Data Breach is confirmed, **"activity 3a"** is carried out, the 72 hours within which the Supervisory Authority must be notified, where applicable, commences from this moment. Otherwise, if the event is NOT considered a Data Breach, **"activity 3b"** is carried out.	Data Breach Register (annex I -*Data Breach Register*)
3a	Data Manager	Summoning of the PIRT	Once the presence of a Data Breach has been ascertained and it has been verified which Group Company(ies) is/are impacted as Data Controllers, the Data Manager sends an official notification to the PIRT (and therefore to the relevant Compliance Manager(s)) and arranges a meeting so as to carry out the necessary analysis, as well as to: • decide whether to request further clarifications or information from the Incident Reporter; • confirm the preliminary assessment carried out by the Data Manager, or not; • determine whether the breach is such as to present a risk to the rights and freedoms of natural persons, and the actions needed to remedy or mitigate the risks. **This activity must be carried out within 24 hours after confirmation that a Data Breach has occurred.**	
3b	Data Manager	Archive the file	Archives the file when the event is NOT considered a Data Breach, i.e. when there is no knowledge or belief that there has been improper or unauthorised collection, access, modification, loss and/or exposure of personal data. Forwards the documentation of what occurred – including the relevant circumstances, consequences and measures taken – to SECUR for entry in the Data Breach Register used to identify and describe 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.	Data Breach Register (annex I -*Data Breach Register*)

3.3.2 Phase II A: Resolution and limitation of effects

As provided for by EU Regulation 2016/679 Article 33, the Data Controller must implement appropriate measures to remedy the personal data breach, stop the effects of the breach and assess the possibility of reducing the effects on 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 its negative effects
- 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.

The table below describes the activities pertaining to the **resolution and limitation of effects phase:**

ID	Role/Person in Charge	Assets	Activity Description	Instruments
4	PIRT	Definition of remedial actions to limit the effect	Definition of the corrective actions plan which contains the actions to be taken to resolve the critical issues caused by the incident and reduce the consequent negative effects.	
5	Data Manager	Implement the actions envisaged by the Remediation Plan to limit the effects	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 (annex 1- *Report Template*) Data Breach Register (annex 1 -*Data Breach Register*)
6	Security Department	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 corrective 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 1 -*Data Breach Register*)

3.3.3 Phase II B: 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."*

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

ID	Role	Assets	Activity Description	Instruments
7	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: • Type of personal data processed; • Volumes of data processed; • Persistence of the personal data in the system;	Data Breach Register (annex 1 -*Data Breach Register*)

ID	Role	Assets	Activity Description	Instruments
			• 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;	
8	PIRT	Assessment of severity of the breach	The PIRT assesses the risk to the rights and freedoms of natural persons (in terms of damage, both pecuniary and non-pecuniary) by means of the "Breach Severity Assessment Methodology", structured according to the ENISA guidelines[9]. 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. The PIRT can also use the instruments provided by the Italian Data Protection Authority for the purposes of the so-called "self-assessment for notification of a personal data breach"[10], pursuant to Article 33 of the GDPR.	Methodology for assessing the severity of a personal data breach (see *Annex I – Severity Assessment Methodology*)
9	PIRT	Report Data Breach Notification Template	The PIRT draws up the report indicating the information required by Article 33, subsection 3 of the GDPR and fills in the template provided by the Italian Data Protection Authority for notification of the breach. The report includes: • 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; • assessment of whether a risk or high risk exists based on the criteria of the Guidelines WP250rev.01[11] **This activity must be performed within 36 hours of calling the PIRT.**	Data Breach Report containing the Remediation Plan (see *Annex I —Template report*) and communication template provided by the Italian Data Protection Authority

[9] European Network and Information Security Agency

[10] Accessible from the web page https://servizi.gpdp.it/databreach/s/

[11] The 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	Assets	Activity Description	Instruments
10	Privacy Compliance Officer	Formalises the severity of the data breach and orders the notification to be sent to the Italian Data Protection Authority	Formalises the severity assessment of the data breach conducted according to the ENISA model: - confirms the report, approving submission of the notification to the Italian Data Protection Authority and, where appropriate, communication of the breach to the data subjects; or - does not confirm the report, indicating the reasons to be documented in the dedicated register. May, in any case request, where necessary, further clarifications or additions. It should be noted that the validated assessment is reported in the final version, in the Data Breach Register, together with the completed Template for sending the notification to the Italian Data Protection Authority. **This activity must be carried out within 12 hours after receipt of the report made by the PIRT**	Data Breach Register (annex 1 -*Data Breach Register*)

With reference to the notification to the data subject, according to the provisions of EU Regulation 2016/679 and WP250 "Guidelines on personal data breach notification pursuant to Regulation (EU) 2016/679", this **is not required** if one of the following conditions is met:

- 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, so that it must be made via a public disclosure or a similar measure by means of which the data subjects are informed in a similarly effective manner.

3.3.4 Phase III: Notification

In line with the provisions of Article 33, subsection 3 of the GDPR, **at the end of the Data Breach assessment** and in any case within the timeframe laid down by the Regulation (72 hours from the time of becoming aware of the breach), the following activities must be carried out:

- **Notification to the Italian Data Protection Authority**: the DPO fills in the dedicated notification template provided by the Data Protection Authority and sends it to the latter (https://servizi.gpdp.it/databreach/s/), filling in the information from the Form approved by the Compliance Manager.[12]
- **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, describing the nature of the breach and providing at least the information and measures referred to in art. 33 paragraph 3 letters b), c) and d) of the GDPR.

[12] If the breach involves data referring to several Group Companies (Data Controllers), the notification must be made by all Data Controllers.

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

ID	Role/Person in Charge	Assets	Activity Description	Instruments
11	DPO	Inform the Data Protection Authority within 72 hours **(if the risk is Very High / High / Average)**	Fills in the dedicated Data Breach report template available on the official website of the Data Protection Authority (in cases of average, high and very high risk to the rights and freedoms of natural persons). 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
12	DPO	Inform the data subject **(if the risk is Very High or High)**	Informs the data subject without undue delay (by email or registered letter) in cases where there is a high or very high risk to the rights and freedoms of the data subject, having made sure that communication is actually required (see subsection 3.3.3). Specifically, the notification contains: - 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, certified e-mail or registered letter

3.3.5 Phase IV: Post Incident Review

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

The following table describes the activities of the **Post Incident review phase**:

ID	Role/Person in Charge	Assets	Activity Description	Instruments
13a	Security Department	Supplement the Data Breach report with the incident closure	Based on the series of assessments of the Data Incident carried out by the PIRT, it is responsible for supplementing the Data Breach summary report with a complete description of the Incident, root causes, lessons learned, opportunities for improvement. It forwards the Report to the Privacy Compliance Manager.	Data Breach Incident Report (Annex I – *Template Report*)

ID	Role/Person in Charge	Assets	Activity Description	Instruments
13b	Privacy Compliance Officer	Review and finalisation of the Data Breach Report	Checks and approves the Report, sends it 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 1 – *Template Report*)
14	Security Department	Update the Data Breach Register	Once the Privacy Compliance Manager has validated the Data Breach Report, the Register is updated with a full description of the corrective actions so as to keep track of what happened in the system and to be able to reconstruct the event if need be.	Data Breach Register (annex 1 -*Data Breach Register*)

4 CONSERVATION, DOCUMENTATION AND RESPONSIBILITY FOR UPDATES

The Security department files the documentation produced by the PIRT in relation to the activities of:

- Definition of remedial actions and containment of the effects of the breach;
- Collection of information concerning the breach and related severity assessment;
- The Data Breach report prepared by the PIRT following the severity assessment of the privacy incident.
- All work documentation arising from the application of this document is filed by the relevant Departments, in accordance with the timeframes and procedures laid down by the Italgas Enterprise System and in any case for no longer than 10 years after the event occurred.

5 LIST OF ANNEXES

Annex		Update Manager
1	Support file Data Breach Management	Security Department