Italgas

Investiamo nel futuro dal 1837

Standard di Compliance

Data Breach Management

Codifica documento: ITH-STC-077-R01

Data emissione: 27/03/2024
Macro-Processo: Compliance
Processo: Compliance data protection
Sottoprocesso: Data breach management

Redatto	SECUR					
Verificato	IGLEGAL	REISAR	CYBSEC (BLU)	ORG&HROP	COMPLA	QUAL
	RELESOST	DPO				
Approvato	AD					
Elementi di Compliance	GDPR[1]					

Storico delle revisioni

- Rev. 01 - Principali modifiche:
  - Inserimento dei riferimenti alle Linee Guida adottate dallo European Data Protection Board (EDPB) il 14 dicembre 2021;
  - Miglioramento dell'accountability attraverso l'inserimento della Fase II A dedicata alla risoluzione e contenimento degli effetti dal data breach e la precisazione circa ruoli e responsabilità specifiche per il processo di data breach management dei Responsabili dell'Osservanza, dei Dati e del Gestore del Contratto.;
  - Recepimento di modifiche organizzative.
- Rev. 00 (25/03/2019)

[1] GDPR General Data Protection Regulation 2016/679

INDICE

1 ABSTRACT

Il presente standard, relativo alle attività di Data Protection, si colloca nell'ambito delle attività di direzione e coordinamento esercitata dalla Capogruppo Italgas S.p.A.
Il documento si rivolge a tutte le Società del Gruppo Italgas, titolari o responsabili del trattamento di dati personali, che sono individualmente ed autonomamente obbligate al rispetto dei requisiti di compliance imposti dalle norme e dai regolamenti applicabili in materia di protezione dei dati personali, ed in particolare di violazione dei dati personali, ed alle funzioni e/o soggetti che al loro interno cooperano in maniera integrata come attori nel processo di gestione delle violazioni.

Per "*violazione dei dati personali*" (in inglese "*data breach"*) si intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Titolari e responsabili delle attività di trattamento sono tenuti ad una serie di adempimenti volti a garantire la tempestiva presa in carico degli incidenti, la gestione dei potenziali effetti che tali incidenti possono determinare sui soggetti interessati e la trasparenza nei confronti dell'Autorità di controllo e dei soggetti interessati stessi.

In particolare, vi è obbligo da parte del titolare di notificare all'Autorità di controllo le violazioni senza ingiustificato ritardo, ove possibile entro 72 ore dalla conoscenza dell'evento, ad eccezione dei casi in cui sia improbabile che la violazione presenti un rischio per i diritti e le libertà dei soggetti interessati.
Nei casi di probabile alto rischio la violazione deve essere comunicata anche ai soggetti interessati.
Tale obbligo, per i responsabili, implica la necessità di segnalare tempestivamente ai titolari tutti gli incidenti che possono costituire violazione di dati personali, in quanto ogni violazione di dati personali risulta essere un caso specifico di incidente di sicurezza[2].

A fronte di quanto sopra descritto, ne consegue la necessità di adottare misure tecniche ed organizzative per essere in grado di individuare, valutare e gestire in maniera rapida ed efficace i casi di potenziale violazione.
Lo standard si propone quindi di rispondere all'esigenza di garantire, nei tempi e con le modalità previste, l'individuazione, la valutazione e l'eventuale notifica dei casi di violazioni dei dati personali di cui le società del gruppo titolari dei trattamenti siano venute a conoscenza, attraverso:

- la definizione di un processo che preveda attività, ruoli, e responsabilità necessari per coordinare in maniera efficace le fasi di gestione dei casi di violazione di dati personali;
- la definizione di strumenti per guidare le unità organizzative coinvolte nel processo di "Data Breach Management" in questo processo.

[2] per quanto concerne gli incidenti di sicurezza si deve fare riferimento anche allo standard di compliance ITH-STC-057 "Business continuity e gestione delle emergenze e della crisi"

2 FUNZIONI COINVOLTE

Funzione Citata nel presente documento	Unità Organizzativa
Funzione Security	Group Security & Real Estate (SECUR)

Per la gestione delle fasi successive di valutazione dei casi specifici, è costituito il "Privacy Incident Resolution Team" (PIRT), formato da:

- Responsabile dell'Osservanza della Società coinvolta nel «Privacy Incident»
- Responsabili dei dati coinvolti nel «Privacy Incident»
- Responsabile Unità General Counsel (IGLEGAL);
- Responsabile Unità HR Business Regolati (HR-REG);
- Responsabile Unità HR Business non Regolati (HR-NR);
- Responsabile Unità Group Security & Real Estate (SECUR);
- Responsabile Relazioni Istituzionali e Affari Regolatori. (REISAR);
- Responsabile Relazioni Esterne e Sostenibilità (RELESOST);
- Responsabile Unità Cybersecurity (CYBSEC) di Bludigit S.p.A.;
- Data Protection Officer (DPO);

Il PIRT assume le decisioni inerenti alla gestione del «Privacy Incident», effettua la valutazione dei rischi per gli interessati rispetto alla violazione accaduta, definisce un piano di azione adeguato alla risoluzione della stessa. Le riunioni del PIRT possono tenersi anche a distanza tramite collegamento audio/video.

Il Responsabile dell'Osservanza può invitare a partecipare alla riunione del PIRT rappresentanti di altre funzioni quando lo ritenga opportuno, in particolare nel caso di assenza/irreperibilità di uno o più dei componenti del PIRT medesimo.

Con ruolo di supporto sono altresì coinvolti:

- Team Data Protection
- Referenti di linea
- Amministratori di sistema

In coerenza con il Modello Organizzativo Data Protection, che definisce ruoli e responsabilità, declinati dallo Standard di Compliance "Data Protection"[3] e assegnati secondo le modalità in quest'ultimo definite, nell'ambito del processo di Data Breach Management ruoli e responsabilità dei principali soggetti coinvolti sono così definiti:

- il **Responsabile dell'Osservanza** formalizza la gravità dei privacy incident, dispone l'invio della notifica al Garante ed esegue una post incident review per valutare la gestione dell'incidente;
- il **Responsabile dei Dati** deve comunicare al PIRT l'eventuale presenza di un privacy incident, effettuarne una valutazione preliminare ed adottare conseguentemente adeguate azioni di rimedio;
- il **Gestore del contratto**, nei casi ove l'incident reporter sia un fornitore esterno, deve richiedere la compilazione del template predisposto e trasmetterlo al Responsabile dei Dati.

Può essere chiamata a supporto del Processo di Data Breach Management ogni altra funzione del Gruppo al fine di garantire il corretto svolgimento delle attività operative.

3 PRINCIPI DI COMPLIANCE

3.1 Obiettivo e prescrizioni generali

L'obiettivo del processo di Data Breach Management è quello di:

- gestire le segnalazioni di potenziali eventi di Data Breach e confermare la presenza di Privacy Incident;
- valutare la gravità della violazione, sulla base della metodologia definita e riportata in allegato al presente documento (*Allegato 1 – Metodologia valutazione gravità*), al fine di stimare il potenziale rischio per i diritti

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

e le libertà fondamentali delle persone fisiche. Tale valutazione è necessaria per stabilire se procedere o meno con la notificazione all'Autorità Garante ed eventualmente agli interessati coinvolti.
- garantire che ogni Titolare notifichi la/le violazione/i alla Autorità di Controllo, ove necessario, e agli interessati nei tempi stabiliti.

La notifica della violazione alla Autorità di Controllo deve avvenire, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui se ne sia venuti a conoscenza, ossia dal momento in cui il Responsabile dei Dati accerta la presenza di un "Privacy Incident", cioè una violazione di dati personali che può presentare un rischio per i diritti e le libertà delle persone fisiche. Qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, il Titolare è tenuto a notificare la violazione anche ai soggetti interessati, senza indebito ritardo[4].
Ai sensi dell'art. 33 comma 1 del GDPR, le società del Gruppo Italgas non sono tenute ad effettuare la notifica all'Autorità se, a valle delle analisi effettuate, risulta che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Ciononostante, si dovrà ugualmente tenerne traccia documentata all'interno del Registro dei Data Breach.
In caso di violazioni più complesse, per stabilire appieno la natura della violazione il titolare del trattamento potrà effettuare una notifica per fasi[5]. Essa prevede entro 72 ore di effettuare una notifica preliminare all'Autorità che contenga le informazioni fino ad allora raccolte sul Privacy Incident e l'indicazione dei motivi del ritardo, in conformità all'articolo 33, paragrafo 1, effettuando quindi una comunicazione successiva alle 72 ore con informazioni supplementari. Inoltre, nel caso in cui la violazione dei dati personali possa generare un rischio elevato per i diritti e le libertà delle persone fisiche, le società del Gruppo Italgas (in qualità di Titolari del trattamento) dovranno comunque darne comunicazione all'interessato senza ingiustificato ritardo.
Nel caso in cui il Gruppo Italgas abbia affidato dei servizi ad un fornitore, quest'ultimo dovrà segnalare tempestivamente ogni evento anomalo ad un referente interno dell'organizzazione, così come indicato nello standard di compliance "Business Continuity e gestione delle emergenze e della crisi"[6]; tale referente interno è identificato nel Gestore del contratto.
Una specifica clausola in merito deve essere inserita negli accordi contrattuali con il fornitore ex art. 28 GDPR affinché sia garantito l'obbligo di informazione di ogni violazione di dati personali da parte del responsabile nei confronti del titolare, così come richiesto dall'art. 33 del GDPR.

3.2 Classificazione ed esempi di violazioni dei dati personali

Per "*violazione dei dati personali*" (in inglese "*data breach"*) si intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"[7].

Secondo quanto previsto dal WP250 "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679", gli eventi di possibile Data Breach («Privacy Incident») possono essere suddivisi in tre macrocategorie:
- "**Violazione di confidenzialità**": in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "**Violazione di disponibilità**": in caso di perdita accidentale o non autorizzata dell'accesso ai dati o la distruzione di dati personali;
- "**Violazione di integrità**": in caso di alterazione non autorizzata o accidentale dei dati personali.

A titolo esemplificativo e non esaustivo vengono riportate di seguito alcune tipologie di violazione dei dati personali:
- **distruzione accidentale di dati informatici o documenti cartacei** intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi, conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato o fisico, rottura di dispositivi di memorizzazione informatica, incendio/allagamento di locali dove sono archiviati i contratti ed altri documenti);

[4] L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi da eventuali conseguenze negative della violazione. Rif. GDPR, cons. 86.
[5] WP250rev.01 "Guidelines on Personal Data Breach Notification Under Regulation"; GDPR, art. 33, p. 4
[6] Standard di compliance ITH-STC-057 "Business continuity e gestione delle emergenze e della crisi"
[7] GDPR, art. 4, p. 12

- **perdita di dati**, conseguente a smarrimento/furto di supporti informatici (es. Laptop, Hard Disk, Memory Card) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- **accesso non autorizzato o intrusione a sistemi informatici** inteso come lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. user ID e password) per l'accesso ai sistemi;
- **modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o da interventi umani;
- **rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati.

Ad integrazione delle Linee Guida WP250 si annoverano ulteriori Linee Guida che riflettono le esperienze comuni delle Autorità Garanti europee dal momento in cui il GDPR è diventato applicabile, tra queste le Linee Guida 01/2021 "Examples regarding Personal Data Breach Notification", adottate dallo European Data Protection Board (EDPB) il 14 dicembre 2021, versione 2.0. Lo scopo di questo documento è di aiutare i titolari del trattamento dei dati a decidere come gestire le violazioni dei dati e quali fattori considerare durante la valutazione del rischio.

3.3 Modalità operative per la gestione delle violazioni

Il presente paragrafo illustra in dettaglio le istruzioni operative da seguire in caso di identificazione di un potenziale Privacy Incident. In particolare, per ogni fase sono mostrate le seguenti informazioni:

- **Checklist/Tabelle** che descrivono le azioni che devono essere compiute e l'Owner dell'attività nelle colonne "Ruolo/Incaricato", "Attività", "Descrizione dell'attività";
- **Materiale di supporto** rappresentato da tutti i documenti a cui si fa riferimento all'interno delle checklist/tabelle nella colonna "Strumenti".

Il processo si sviluppa secondo le fasi standard sotto descritte. Si ribadisce che i requisiti di compliance imposti dalle norme applicabili gravano in maniera diversa sulle società del Gruppo nel caso in cui siano esse stesse singolarmente titolari dei trattamenti dei dati ai quali la violazione si riferisce, oppure responsabili del trattamento. Nel primo caso l'obbligo di notifica è in capo ad ogni società titolare, nel secondo non vi è un obbligo di notifica ma solo di comunicazione tempestiva ai titolari.

- **Fase I - Identificazione**: identificare, tramite una valutazione preliminare, se le segnalazioni ricevute possano essere definite come Privacy Incident;
- **Fase II A – Risoluzione e contenimento effetti:** implementare il piano di azione correttiva con l'obiettivo di mitigare il rischio individuato e predisporre delle tempestive azioni in modo da contenere e gestire al meglio il Privacy Incident individuato;
- **Fase II B - Valutazione:** effettuare la valutazione della rilevanza del Privacy Incident, tramite la stima del potenziale rischio associato ai diritti e libertà delle persone fisiche. Tale attività è fondamentale per stabilire se notificare o meno il Data Breach all'Autorità Garante ed eventualmente agli interessati coinvolti;
- **Fase III - Notifica:** formalizzare il report e se opportuno comunicare il report medesimo alle società del Gruppo titolari del trattamento. Se necessario notificare all'autorità Garante l'avvenuto Data Breach tramite l'apposito servizio online e, nei casi ove previsto, comunicarlo all'interessato;
- **Fase IV - Post Incident review:** svolgere un esame ex post della gestione del Privacy Incident, al fine di predisporre un report di chiusura dell'Incident.
  Tale report deve essere inviato ai Responsabili dei Dati coinvolti e deve comprendere:
  - le principali cause dell'evento;
  - le azioni implementate per superare le criticità emerse;
  - eventuali opportunità di miglioramento dei processi aziendali.

Di seguito una rappresentazione del processo di gestione Data Breach sotto forma di diagramma di flusso.

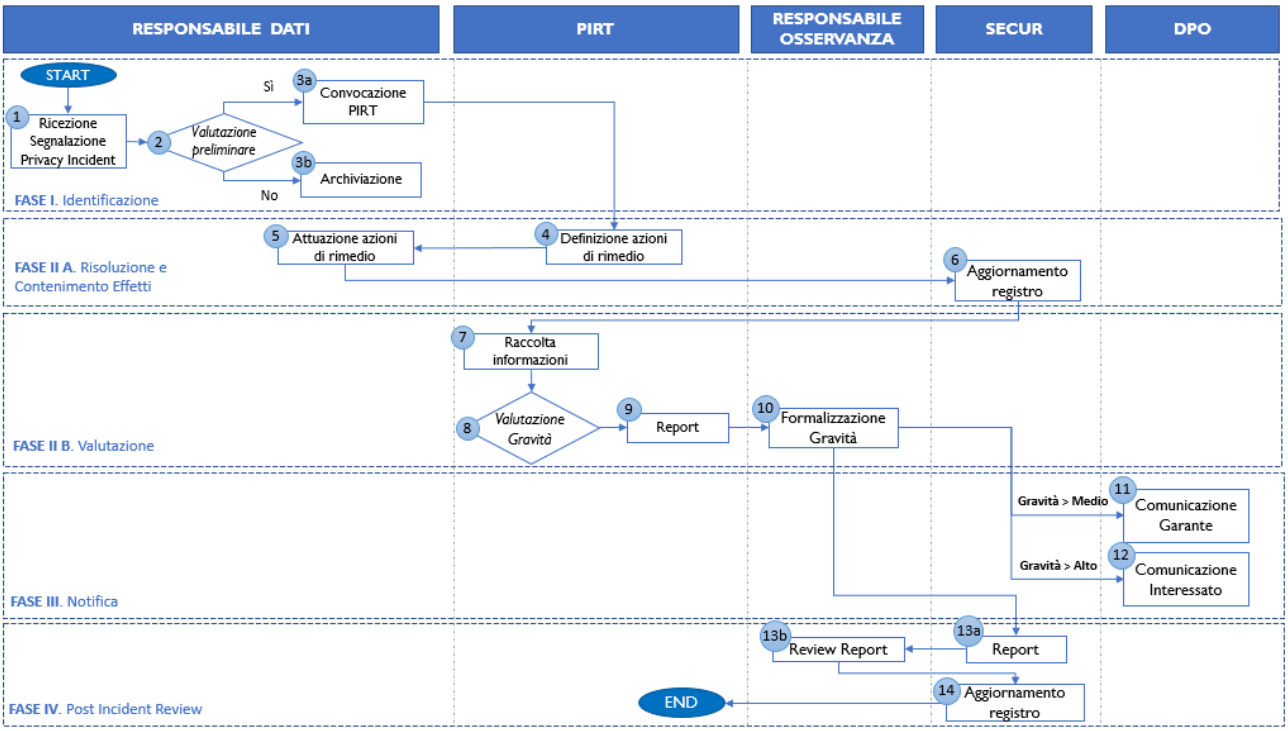

Figura 1: processo di gestione Data Breach

3.3.1 Fase I: Identificazione

La conoscenza del verificarsi di una situazione anomala può emergere a fronte di segnalazioni che possono provenire da diverse fonti:

- dalle **funzioni IT**, nell'ambito delle loro attività di monitoraggio della sicurezza: si tratta di situazioni di perdita di integrità, disponibilità, riservatezza di dati di carattere personale, che possono quindi avere determinato un potenziale impatto sui soggetti ai quali sono riferiti i dati;
- da **un fornitore esterno** oppure una Società del Gruppo, nominati responsabili per il trattamento dei dati. In questi casi la segnalazione avviene attraverso la compilazione di un apposito modello allegato alla presente procedura con i tempi e le modalità definite con il contratto di nomina ex art. 28;
- da un **dipendente:** viene segnalato ad esempio il furto o lo smarrimento di un dispositivo mobile (es. chiavetta USB, hard disk, telefono cellulare, tablet o laptop) contenente dati personali;
- da altre **fonti esterne** quali possono essere l'**Autorità di controllo**, dai **soggetti interessati stessi**, dai **media** o **altri canali esterni**.

Tutte le segnalazioni di possibili violazioni di dati personali, ricevute tramite mail o alert di sistema dai dipendenti/collaboratori esterni/clienti o dai fornitori, devono essere inoltrate ai Responsabili dei Dati di riferimento per il trattamento posto in essere.
Il Responsabile dei Dati ne effettua una valutazione preliminare, che avrà l'obiettivo di confermare o meno il Privacy Incident.

Le segnalazioni con rilevanza privacy sono trasmesse dal Responsabile dei Dati al PIRT e vengono registrate da SECUR nel Registro Data Breach[8].

I dipendenti sono tenuti a segnalare le possibili violazioni di dati personali ai Responsabili dei Dati di riferimento per il trattamento posto in essere. Le istruzioni nei contratti con i fornitori prevendono l'obbligo di riferire al Titolare eventuali violazioni di dati personali contattando il gestore del contratto. Infine, gli interessati possono contattare il DPO all'indirizzo e-mail presente in tutte le informative.

[8] Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, il titolare del trattamento deve conservare la documentazione di tutte le violazioni. Egli è tenuto a registrare i dettagli relativi alla violazione, comprese le cause, i fatti, e i dati personali interessati.

Nella tabella seguente sono descritte le attività inerenti alla **fase di identificazione:**

ID	Ruolo	Attività	Descrizione Attività	Strumenti
1	Incident Reporter (dipendenti/ collaboratori esterni/ fornitori/altre fonti)	Identificazione e segnalazione del Privacy Incident	Identifica un potenziale Privacy Incident inviando una segnalazione nelle seguenti casistiche: • Se l'Incident Reporter è un fornitore esterno (Responsabile del trattamento), il Gestore del contratto gli richiede la compilazione del template predisposto (inserito nell'allegato 1) e trasmette immediatamente la segnalazione al Responsabile dei Dati di riferimento; • Se l'Incident Reporter è un dipendente deve comunicarlo al Responsabile dati del trattamento posto in essere; • Qualora la segnalazione venga effettuata tramite altro canale da un soggetto esterno (es. soggetto interessato, media...), questa deve essere prontamente inoltrata al Responsabile dei Dati di riferimento. In caso di assenza/irreperibilità del Responsabile dei dati, la comunicazione deve essere indirizzata al Responsabile dell'Osservanza.	Template Comunicazione Data Breach da parte del Responsabile del trattamento (allegato 1 – *Template Comunicazione)*
2	Responsabile dei dati	Ricezione dell'Alert di Sistema/mail di segnalazione, valutazione preliminare e creazione fascicolo e conferma della presenza di un Privacy Incident	Riceve la segnalazione, effettua una valutazione preliminare raccogliendo tutte le informazioni circa l'evento occorso e provvede alla creazione di un fascicolo volto a verificare la sussistenza di un data breach. Può richiedere il supporto del DPO e delle Funzioni Compliance IT e Cybersecurity. Nel caso di conferma della presenza di un Data Breach si procede con **"l'attività 3a"**, da questo momento decorrono le 72 ore entro cui effettuare, ove necessaria, la notifica alla Autorità di Controllo. Nel caso contrario, ossia l'evento NON viene considerato un Data Breach, si procede con **"l'attività 3b".**	Registro dei Data Breach (allegato 1 - *Registro Data Breach*)
3a	Responsabile dei dati	Convocazione del PIRT	Appurata la presenza di un Data Breach e verificata quale/i Società del Gruppo impatta come Titolarità, il Responsabile dei dati invia comunicazione ufficiale al PIRT (e dunque al/ai relativo/i Responsabile dell'Osservanza) e lo convoca al fine di effettuare le analisi necessarie, nonché per: • valutare se richiedere ulteriori chiarimenti o informazioni all'Incident Reporter; • confermare o meno la valutazione preliminare svolta dal Responsabile dei Dati; • determinare se la violazione sia tale da presentare un rischio per i diritti e le libertà delle persone fisiche, e le azioni necessarie per porvi rimedio, o attenuare i rischi. **Tale attività deve essere eseguita entro 24 ore dalla conferma della presenza del Data Breach.**	
3b	Responsabile dei dati	Archiviare il fascicolo	Archivia il fascicolo quando l'evento NON viene considerato un Data Breach ovvero quando non vi è conoscenza o convinzione che ci sia stata raccolta, accesso, modifica, perdita e/o esposizioni di dati personali in maniera impropria o non autorizzata. Trasmette a SECUR la documentazione relativa a quanto avvenuto – comprese le circostanze relative, le conseguenze e i provvedimenti adottati – per l'annotazione nel Registro Data Breach, dedicato all'individuazione e alla descrizione delle violazioni dei dati personali. Nel caso in cui l'evento non sia considerato un Data Breach verrà gestito come gli altri Incidenti di sicurezza come definito nelle policy di Gruppo.	Registro dei Data Breach (allegato 1 - *Registro Data Breach*)

3.3.2 Fase II A: Risoluzione e contenimento effetti

Secondo quanto previsto dal Regolamento UE 2016/679 art. 33, il Titolare deve mettere in atto adeguate misure per porre rimedio alla violazione dei dati personali interrompendo gli effetti della violazione e valutando la possibilità di ridurre gli effetti per i soggetti interessati.
Nello specifico il "Remediation Plan" dovrà contenere:

- le azioni organizzative e tecnologiche che saranno intraprese per rispondere alla violazione al fine di attenuarne gli effetti negativi
- i ruoli e le responsabilità del personale designato per mettere in atto le azioni di rimedio;
- un Gantt volto ad individuare tempi e costi delle azioni di rimedio.

Nella tabella seguente sono descritte le attività inerenti alla **fase di risoluzione e contenimento effetti:**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
4	PIRT	Definizione azioni di rimedio per contenimento effetto	Definisce il piano di azioni correttive, contenente le azioni da intraprendere al fine di risolvere le criticità causate dall'incidente e ridurre gli effetti negativi prodotti.	
5	Responsabile dei Dati	Attuare le azioni previste dal Remediation plan per contenimento effetti	Attua il piano di azioni correttive, contenente le azioni da intraprendere al fine di risolvere le criticità legate all'Incident evidenziato.	Report sul Data Breach contenente il Remediation plan (allegato 1- *Template Report*) Registro dei Data Breach (allegato 1 - *Registro Data Breach*)
6	Funzione Security	Aggiornare il Data Breach sul Registro	Una volta completata l'azione correttiva aggiorna il registro Data Breach riportando una descrizione completa dell'evento e delle azioni correttive in modo da tenere traccia a sistema di quanto accaduto e di potere ricostruire l'evento nel caso fosse necessario.	Registro dei Data Breach (allegato 1 - *Registro Data Breach*)

3.3.3 Fase II B: Valutazione

Secondo quanto previsto dal Regolamento UE 2016/679 art. 33 *"Il titolare del trattamento documenta **qualsiasi violazione** dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo."*

Nella tabella seguente sono descritte le attività inerenti alla **fase di valutazione:**

ID	Ruolo	Attività	Descrizione Attività	Strumenti
7	PIRT	Raccolta informazioni sulla natura del Data Breach	Raccoglie ulteriori informazioni sulla natura del Data Breach e le inserisce nel Registro dei Data Breach, nell'ottica di classificare la natura del dato violato e di tenere traccia della violazione. In particolare, raccoglie le seguenti informazioni sull'evento occorso: • Tipologia di dato personale trattato; • Volumi di dati trattati; • Persistenza del dato personale sul sistema; • Completezza del dato personale trattato; • Intelligibilità del dato trattato;	Registro dei Data Breach (allegato 1 - *Registro Data Breach*)

ID	Ruolo	Attività	Descrizione Attività	Strumenti
			• Numero di utenti autorizzati all'accesso al dato; • Posizionamento sulla rete del sistema che tratta il dato; • Misure di sicurezza in essere volte alla mitigazione del rischio;	
8	PIRT	Valutazione della gravità della violazione	Il PIRT effettua la valutazione del rischio per i diritti e le libertà delle persone fisiche (in termini di danno, patrimoniale e non patrimoniale) tramite la "Metodologia di valutazione della gravità della violazione", strutturata in base alle linee guida ENISA[9]. Tale valutazione è fondamentale per comprendere se procedere o meno con la notificazione all'Autorità Garante e/o agli interessati coinvolti. Il PIRT può avvalersi altresì degli strumenti che il Garante per la protezione dei dati personali mette a disposizione ai fini della c.d. "Auto valutazione per la notifica di una violazione dei dati personali (data breach)"[10], ex art. 33 del GDPR.	Metodologia di valutazione della gravità della violazione dei dati personali (riferimento all'*Allegato 1 – Metodologia valutazione gravità*)
9	PIRT	Report Data Breach Modello di Notifica	Il PIRT redige il report indicando le informazioni richieste dall'art. 33 par. 3 del GDPR e compila il modello predisposto dal Garante per la notifica della violazione. Il report include: • la descrizione della violazione, delle categorie e del numero di interessati coinvolti; • la descrizione delle probabili conseguenze, con indicazione del grado di probabilità che il Data Breach presenti un rischio per i diritti e le libertà delle persone fisiche; • la descrizione delle misure immediate da adottare o delle quali proporre l'adozione; • una valutazione dell'esistenza di un rischio o di un rischio elevato, in base ai criteri delle Linee Guida WP250rev.01[11] **Tale attività deve essere eseguita entro le 36 ore successive alla convocazione del PIRT.**	Report sul Data Breach contenente il Remediation plan (riferimento all'*Allegato 1 - Template report*) e Modello per la comunicazione predisposto dal Garante
10	Responsabile dell'Osservanza	Formalizza la gravità della violazione del Data Breach e dispone l'invio della notifica al Garante	Formalizza la valutazione della gravità della violazione del Data Breach effettuata secondo il modello ENISA: - confermando la relazione, approvando l'invio della notifica al Garante e, se del caso, della	Registro dei Data Breach (allegato 1 - *Registro Data Breach*)

[9] European Network and Information Security Agency
[10] Accessibile dalla pagina web https://servizi.gpdp.it/databreach/s/
[11] La valutazione del rischio deve contenere: tipo di violazione, natura, e volume dei dati, facilità di identificazione degli interessati, gravità delle conseguenze per gli interessati, particolari caratteristiche degli interessati, numero di interessati colpiti, particolari caratteristiche del titolare del trattamento.

ID	Ruolo	Attività	Descrizione Attività	Strumenti
			comunicazione della violazione agli interessati; oppure - non confermando la relazione, indicandone le ragioni da documentare nell'apposito registro. In ogni caso può chiedere, ove necessario, ulteriori chiarimenti o integrazioni. Si specifica che la valutazione validata viene riportata sulla versione definitiva del Registro dei Data Breach, unitamente al Modello compilato per l'invio della notifica al Garante. **Tale attività deve essere eseguita entro 12 ore dalla ricezione del report svolto dal PIRT**	

Con riferimento alla comunicazione all'interessato, secondo quanto previsto dal Regolamento UE 2016/679 e dal WP250 "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679", la stessa **non è richiesta** se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- se il titolare del trattamento ha adottato misure successive alla violazione che garantiscano la riduzione del rischio per i diritti e le libertà degli interessati;
- se la notifica all'interessato comporta sforzi sproporzionati, per cui deve essere effettuata tramite una comunicazione pubblica o una misura simile per la quale gli interessati vengano informati in modo altrettanto efficace.

3.3.4 Fase III: Notifica

In linea con quanto previsto dall'art. 33 par. 3 del GDPR, **al termine della valutazione del Data Breach** e comunque nei termini previsti dal Regolamento (72 ore dal momento in cui se ne sia venuti a conoscenza), devono essere svolte le seguenti attività:

- **Notifica al Garante:** il DPO compila l'apposito modulo di segnalazione predisposto dall'Autorità Garante e lo invia al Garante (https://servizi.gpdp.it/databreach/s/), inserendovi le informazioni riportate sul Modello approvato dal Responsabile dell'Osservanza.[12]
- **Comunicazione all'interessato**: il DPO ha l'onere di comunicare all'interessato la violazione dei suoi dati personali in un linguaggio semplice e chiaro, descrivendone la natura e riportando almeno le informazioni e le misure di cui all'art. 33 par. 3 lett. b), c) e d) del GDPR.

Nella tabella seguente sono descritte le attività inerenti alla **fase di notifica:**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
11	DPO	Notificare all'autorità Garante entro 72 ore **(nel caso il rischio sia Molto Alto/ Alto / Medio)**	Compila apposito modulo di segnalazione dei Data Breach presente sul sito istituzionale dell'autorità Garante (nei casi di rischio per i diritti e le libertà delle persone fisiche medio, alto e molto alto). La notifica del Data Breach deve includere almeno le seguenti informazioni: • la natura della violazione dei dati personali includendo, ove possibile, le categorie e il	Modulo di segnalazione

[12] Nel caso la violazione interessi dati riferibili a più Società del Gruppo (Titolari), la notifica deve essere avanzata da tutti i Titolari.

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
			numero approssimativo di persone interessate e le tipologie e il numero approssimativo di record di dati personali in questione; • il nome e i recapiti del responsabile della protezione dei dati e di eventuali punti di contatto che possano fornire informazioni; • le probabili conseguenze della violazione dei dati personali; • le misure adottate o proposte che devono essere usate dal Titolare per affrontare la violazione dei dati personali, tra cui eventuali misure per attenuarne i possibili effetti negativi. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.	
12	DPO	Comunicare all'interessato **(nel caso il rischio sia Molto Alto o Alto)**	Informa l'interessato senza ingiustificato ritardo (tramite mail, PEC o lettera raccomandata) nei casi di rischio alto o molto alto per i diritti e le libertà dell'interessato, previa verifica dell'effettiva necessità della comunicazione (vedi ultimo periodo del par. 3.3.3). In particolare, la comunicazione contiene: - il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni; - le probabili conseguenze della violazione dei dati personali; - le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.	Mail con conferma di lettura, PEC o lettera raccomandata

3.3.5 Fase IV: Post Incident Review

Dopo la risoluzione si effettua un esame ex post della gestione del Data Breach al fine di predisporre un report di chiusura dell'Incident.

Nella tabella seguente sono descritte le attività della **fase di post Incident review**:

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
13a	Funzione Security	Integrare il report sul Data Breach con la chiusura dell'Incident	Sulla base del complesso delle valutazioni sul Data Incident effettuate dal PIRT, ha il compito di integrare il report riepilogativo sul Data Breach con la descrizione completa dell'Incident, le root causes, lessons learned, opportunità di miglioramento. Inoltra il Report al Responsabile dell'Osservanza.	Report sul Data Breach Incident (allegato 1 - *Template Report*)
13b	Responsabile dell'Osservanza	Review e finalizzazione del Report sul Data Breach	Verifica e approva il Report, lo invia ai Responsabili delle Funzioni aziendali coinvolte nella violazione. Tale report contiene: • descrizione completa dell'evento • azioni di mitigation • esito e chiusura dell'Incident Lo stesso viene presentato in occasione del CdA, OdV e CS.	Report sul Data Breach Incident (allegato 1 - *Template Report*)

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
14	Funzione Security	Aggiornare il Data Breach sul Registro	Una volta che il Responsabile dell'Osservanza valida il Report Data Breach, il Registro viene aggiornato riportando una descrizione completa delle azioni correttive in modo da tenere traccia a sistema di quanto accaduto e di potere ricostruire l'evento nel caso fosse necessario.	Registro dei Data Breach (allegato 1 - *Registro Data Breach*)

4 CONSERVAZIONE DOCUMENTAZIONE

La Funzione Security conserva la documentazione prodotta dal PIRT in relazione alle attività di:

- Definizione azioni di rimedio e contenimento effetti della violazione;
- Raccolta informazioni riguardanti l'avvenuta violazione e la relativa valutazione di gravità;
- Il report sul Data Breach redatto dal PIRT a seguito della valutazione di gravità del privacy incident.
- Tutta la documentazione di lavoro, conseguente all'applicazione del presente documento, è conservata dalle Funzioni competenti, secondo le tempistiche e le modalità previste dall'Italgas Enterprise System e comunque non oltre i 10 anni successivi a quello in cui si è verificato l'evento.

5 ELENCO ALLEGATI

Allegato		Responsabile aggiornamento
1	File di supporto Data Breach Management	Funzione Security