PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

Redatto da		*Verificato da*		*Approvato da*	
Funzione: RSI		*Funzione: DPO- Funzione: Coordinatore Privacy*		*Funzione: DG*	
Data: 12.04.2024	*Firma:*	*Data: 12.04.2024*	*Firma:*	*Data: 12.04.2024*	*Firma:*

REVISIONI			
Riferimenti	Descrizione Aggiornamento	Verifica	Approvazione

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

INDICE

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

1 Scopo e campo di applicazione

La presente procedura regolamenta la gestione degli eventi di Data Breach e la sua finalità è quella di comunicare la modalità di gestione delle segnalazioni che possono portare a situazioni di anomalie/sospetti o di Data Breach.

Si considerano eventi di Data Breach quelli che comportano, in modo accidentale o illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trattati da AIR CAMPANIA S.P.A.

2 Riferimenti

La presente procedura rimanda ai seguenti documenti:

MI 4.4 - A	Manuale Sistema Integrato
GDPR	Regolamento UE 2016/679 "Regolamento generale sulla protezione dei dati personali": ▪ art. 33: Notifica di una violazione dei dati personali all'autorità di controllo; ▪ art. 34: Comunicazione di una violazione dei dati personali all'interessato ▪ Considerando 85-86-87-88 del GDPR
Codice Privacy	Decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali"
Linee Guida	▪ Linee guida 9/2022 in materia di notifica delle violazioni di dati personali (Data Breach) ▪ Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione dei dati

3 Abbreviazioni

Al fine di semplificare l'uso corrente dei termini di utilizzo più frequente vengono indicate le seguenti abbreviazioni:

Sigle di struttura	
AU	Amministratore Unico
DG	Direzione Generale
Team	Data Breach Management Team
DPO	Data Protection Officer
CP	Coordinatore privacy
AdS	Amministratori di Sistema

RP	Referenti privacy

Documenti di processo	
(M01)	Registro incidenti Data Breach
(M02)	Fac simile mod. Comunicazione Data Breach verso il Garante

4 Termini e definizioni

- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Dati particolari (anche cd. "sensibili"):** i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **Dati biometrici:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **Dati giudiziari**: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la

consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- **Violazione dei dati personali:** 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;
- **Pseudonimizzazione:** il trattamento dei dati personali in modo tale che tali dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **Data Protection Officer (DPO):** Responsabile della protezione dei dati ai sensi degli artt. 37-39 del GDPR;
- **Garante**: Autorità Garante per la protezione dei dati personali;
- **Referenti privacy:** persone nominate per supportare i propri Settori /Uffici nelle attività in ambito privacy;
- **Designati:** dipendenti apicali autorizzati dal Titolare (o dal Responsabile) del Trattamento a compiere specifici compiti e funzioni connessi al trattamento dei dati personali;
- **Autorizzati**: chiunque agisca sotto l'autorità diretta del Titolare, del Responsabile del Trattamento e dei Designati ed ha accesso a dati personali nell'ambito dell'attività lavorativa posta in essere per AIR CAMPANIA S.P.A.;
- **Amministratori di sistema:** persone fisiche incaricate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti;

- **Data Breach Management Team:** gruppo composto da diverse funzioni aziendali che assicurano la realizzazione della presente procedura in linea con gli adempimenti normativi previsti dal GDPR;
- **Interessato**: la persona fisica cui si riferiscono i dati personali;
- **Terzi**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità del Titolare o del Responsabile.

5 Responsabilità e Ruoli

Per gestire la crisi conseguente ad un evento di Data Breach è necessario costituire un Data Breach Management Team (di seguito, il "Team"), chiamato a svolgere una funzione di guida in merito alle modalità operative che tutta l'organizzazione dovrà adottare e con particolare riferimento all'attività di comunicazione.

Il Team è composto dalle seguenti figure:

- AU o suo delegato;
- DPO che, di solito, funge da interfaccia con il Garante;
- Coordinatore privacy;
- Referenti privacy;
- Amministratori di sistema.

Altre funzioni saranno coinvolte in base all'evento (Dirigenti; Responsabile della Comunicazione, Responsabile Ufficio Legale, Responsabile gestione documentale, Responsabile transizione digitale, Responsabili esterni, fornitori, ecc.)

6 Modalità Operative

6.1 Gestione evento di *Data Breach* –Segnalazioni

Le segnalazioni potranno essere inoltrate direttamente al Titolare del trattamento ai seguenti indirizzi email: privacy@aircampania.it ovvero alla pec: air@pec.aircampania.it. Eventualmente, le segnalazioni potranno essere inoltrate al DPO alla seguente e-mail: dpo@aircampania.it. Le segnalazioni possono pervenire da canali interni ed esterni

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

Dall'Interno – nel caso si abbia anche soltanto il sospetto di una violazione (sia interna che esterna) di dati o si venga a conoscenza di una comunicazione da parte di un interessato/terzo (anche esterno), ogni dipendente, in quanto persona autorizzata al trattamento nell'area di propria competenza, deve:

- informare il proprio Dirigente-Designato e il Referente Privacy competente e contestualmente inviare la segnalazione al Coordinatore Privacy e/o ad uno dei componenti del Team, della possibile violazione in modo da attivare la procedura di valutazione dell'evento;
- la segnalazione può avvenire con qualsiasi forma, purché avvenga nel minor tempo possibile;
- anche soltanto un sospetto deve essere comunicato al fine di procedere con la valutazione.

Il Coordinatore Privacy, sulla base di un'analisi preliminare dell'accaduto, ravvisati gli estremi per la classificazione quale Data Breach, procede alla convocazione del Team per accertarne l'effettiva sussistenza.

Dall'Esterno (verificare come è stato riscritto il pezzo successivo**)**

Le segnalazioni di un possibile Data Breach possono provenire dall'esterno (interessato/Garante/stampa/responsabile esterno del trattamento, segnalante, etc.) in qualsiasi forma e sono raccolte da DPO, dal Coordinatore Privacy, dai Designati e dai Referenti privacy.

Inoltre, il DPO consulta regolarmente il sito del Garante e gli organi di stampa specializzata per verificare eventuali situazioni di potenziale rischio.

Chiunque riceva la segnalazione dovrà farsi carico, nel più breve tempo possibile, di inviare la stessa al Coordinatore privacy all'indirizzo privacy@aircampania.it o all'indirizzo mail del DPO: dpo@aircampania.it; il Coordinatore Privacy aziendale procederà ad interessare i componenti del Team.

Tutte le comunicazioni che provengono da fonte interna o da fonti esterne devono essere identificate con l'orario e la fonte di provenienza (riportando, quando possibile, documentazione a supporto).

Ad ogni segnalazione è assegnato un numero univoco (ID) formato dal numero progressivo/anno per identificare in modo univoco tutta la documentazione che riguarda l'incidente. Il numero va sempre riportato come riferimento.

Appena ricevuta la segnalazione, il Coordinatore Privacy aggiorna il modulo (M01 – Registro incidenti Data Breach).

6.1.1 Tempistica

Il calcolo della tempistica (considerando che il GDPR fornisce 72 ore al Titolare per la eventuale notifica al Garante, nonché la comunicazione all'interessato senza ingiustificato ritardo) decorre dal momento in cui è venuto a conoscenza della violazione dei dati.

6.1.2 Valutazione di pertinenza della segnalazione raccolta

Tutte le segnalazioni e conseguenti valutazioni vengono registrate e documentati sul modulo (M01 – Registro incidenti Data Breach) da parte del Coordinatore Privacy o suo delegato.

Il Coordinatore Privacy, oppure, in sua assenza, altro membro del Team all'uopo designato, convoca, nel tempo più breve possibile e comunque entro massimo 24 ore dalla segnalazione, una riunione coinvolgendo tutti i membri disponibili ed eventuali altri soggetti potenzialmente coinvolti sulla base delle informazioni disponibili. Qualora qualche membro non fosse disponibile si procede, comunque, con la riunione anche utilizzando canali di comunicazione telematici e virtuali per concertare la gestione del Data Breach.

Il Team, se del caso, procede alla raccolta di ulteriori informazioni (es. richieste di approfondimento), al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato.

6.2 Decisione di non procedere

Qualora fosse accertata, anche dopo eventuali approfondimenti, l'inesistenza di situazioni che mettono a rischio la sicurezza dei dati e le libertà e i diritti degli interessati, previa valutazione del Team, il Coordinatore Privacy registra la decisione nel suddetto modulo M01 (Registro incidenti Data Breach) e comunica formalmente la decisione al Titolare che ha la facoltà, comunque, di richiedere un ulteriore approfondimento.

6.3 Esecuzione Analisi del Rischio e registrazione risultati

In caso di esito positivo (violazione accertata), il Team procede con l'Analisi del rischio e valuta la necessità di avviare eventuali Azioni Correttive, completando la compilazione del modulo M01 - Registro incidenti Data Breach nella quale si deve tenere conto del significato associato a:

- **Riservatezza**: Stima del danno/impatto che la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati comporterebbe per l'interessato;

- **Integrità**: stima del danno/impatto che la perdita di integrità comporterebbe per l'interessato.
- **Disponibilità**: stima del danno/impatto che la perdita di disponibilità comporterebbe per l'interessato.

Dell'esito della decisione si informa il Titolare del Trattamento.

All'esito della valutazione del Team, compete al Coordinatore Privacy riportare l'esito della casistica in cui cade la segnalazione sul modulo M01 - Registro incidenti Data Breach.

6.4 Azioni a seguito delle decisioni

Sulla base della casistica in cui si ricade, debbono essere svolte le seguenti azioni:

Caso A - nessun rischio calcolato

- si aggiorna il modulo M01 - Registro incidenti Data Breach - e si chiude l'evento senza eseguire ulteriori comunicazioni;

Caso B - rischio che implica l'adozione di trattamento dell'evento ed eventuale Azione Correttiva

- si aggiorna il modulo M01 -Registro incidenti Data Breach - e si procede con le eventuali Azioni Correttive comunicando internamente l'adozione delle azioni di trattamento convenute;

Caso C - rischio che implica l'adozione di trattamento dell'evento, l'Azione Correttiva e la notifica obbligatoria all'Autorità di controllo

- si aggiorna il modulo M01 - Registro incidenti Data Breach;
- si procede con l'adozione di azioni Correttive per porre rimedio all'evento anche cercando di attenuarne i possibili effetti negativi;
- si procede con la notifica all'Autorità di controllo nelle forme di cui all'articolo 7.1.

Caso D - rischio che implica, oltre a quanto previsto dal "caso C" anche la comunicazione obbligatoria agli interessati coinvolti

- si prepara apposita comunicazione da trasmettere agli interessati nelle forme di cui al punto 7.2.

Le notifiche all'Autorità del Garante e le comunicazioni obbligatorie agli interessati devono avvenire con tempestività a seguito dall'adozione della decisione e comunque entro le 72 ore. Tanto vale anche per la notifica cd. preliminare al Garante.

6.5 Gestione dell'evento e Azioni Correttive

Quando è prevista un'attività di mitigazione dell'incidente volta a minimizzare gli impatti sui diritti e le libertà degli interessati e, ove possibile, ripristinare la situazione precedente all'incidente, il Team definisce modalità, responsabilità e tempi.

Il Team valuta la necessità di aggiornare la valutazione dei rischi, eventualmente la DPIA se prevista per tale trattamento e la documentazione (es. procedure di riferimento per la nomina a Responsabile esterno del Trattamento).

Il Team monitora lo stato di avanzamento delle azioni di mitigazione previste e tiene aggiornato il modulo M01 - Registro incidenti Data Breach.

6.6 Situazioni anomale o di emergenza

In caso di segnalazioni in situazioni anomale o di emergenza, quali:

- chiusura temporanea delle sedi (es. periodo di ferie),
- assenza di figure apicali del Team,
- assenza di possibilità di collegamento,

devono considerarsi le seguenti misure:

- il Team può operare anche con una sola persona tra quelle che lo compongono;
- le riunioni del Team possono essere tenute in luoghi diversi dalla sede e tramite altre tipologie di strumenti elettronici (conference call, video call).

6.7 Verbalizzazione delle attività

Tutte le attività e le riunioni del Team devono essere documentate ed i verbali sono conservati dal Coordinatore Privacy, responsabile del Team.

Almeno una volta all'anno, il Coordinatore Privacy predispone una relazione sulla attività del Team, trasmessa all'Amministratore Unico di AIR CAMPANIA S.P.A.

La relazione dovrà, per quanto possibile, essere integrata da dati numerici per comprendere l'entità degli eventi ed i tempi di reazione.

6.8 Aspetti decisionali

L'AU deve essere sempre informato degli sviluppi e delle decisioni del Team in ogni fase dell'indagine ed ha potere di imporre misure più restrittive a tutela dei diritti e delle libertà degli interessati.
Qualora l'AU non fosse disponibile a fornire il contributo richiesto, il Coordinatore Privacy è delegato a procedere autonomamente nelle decisioni prese dal Team.
Qualora l'AU non condividesse la decisione presa dal Team e la valutasse eccessiva in quanto ritiene possa impattare negativamente sulla reputazione/immagine dell'Azienda o ledere gli interessi economici della stessa, si assume la responsabilità di imporre la sua decisione.
In questo caso, il Team verbalizzerà la decisione dell'AU, aggiornerà il modulo M01 Registro incidenti Data Breach ed archivierà la documentazione.
Il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti le violazioni dei dati personali ed è sempre autonomo nel prestare le proprie valutazioni. Resta salvo che sul procedere o meno alla notifica al Garante, l'AU potrà discostarsi dalle valutazioni del DPO motivando specificamente le ragioni concrete di tale scelta.
All'occorrenza, possono essere coinvolti esperti esterni che saranno incaricati della valutazione dell'evento previa sottoscrizione di un vincolo di riservatezza.

6.9 Conseguenza dell'evento

Il Team valuta eventuali azioni per contenere gli effetti dell'evento attivando e documentando le risorse e le iniziative necessarie: misure tecniche, informatiche e organizzative.

7 Comunicazioni al Garante e agli interessati

A seguito di un evento di Data Breach, deve essere effettuata la notifica all'Autorità Garante e, nei casi previsti (cfr: 6.5 caso D), anche agli interessati.
La comunicazione è coordinata dal Team. Le evidenze di tutte le comunicazioni devono essere conservate.

7.1 Notifica al Garante

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

La notifica dell'accaduto all'Autorità Garante deve essere inviata nel più breve tempo possibile e comunque entro 72 ore dall'avvenuta conoscenza della violazione. Laddove la notifica sia effettuata oltre tale limite temporale, è necessario dare conto delle relative motivazioni che hanno comportato il ritardo che andranno riportate in apposita verbalizzazione e nel Modulo M01.

Si considera che l'Azienda è "a conoscenza" del Data Breach nel momento in cui vi è contezza che l'incidente di sicurezza ha comportato la compromissione dei dati personali trattati nell'ambito delle proprie attività di trattamento.

Contestualmente alla notifica al Garante, il Coordinatore Privacy aggiorna il modulo M01 - Registro incidenti Data Breach.

7.2 Comunicazione agli interessati

Il Responsabile della Comunicazione, unitamente al Coordinatore Privacy, sentito il DPO, provvede alla predisposizione della comunicazione agli interessati nei casi in cui la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Il contenuto e le modalità di redazione della stessa sono riportati nel paragrafo seguente.

La comunicazione agli interessati, approvata dal Titolare del trattamento, può avvenire con modalità diverse, tra le quali:

- comunicazione diretta agli interessati, ove sia tecnicamente possibile;
- comunicato stampa;
- comunicazione tramite sito WEB/social media;
- altre forme.

7.2.1 Linee Guida per la redazione delle comunicazioni verso gli interessati

Aspetti generali:

- definire il tono della comunicazione che può essere più informale (comunicato) o più formale (dichiarazione ufficiale);
- fornire un titolo "giornalistico" che, per quanto possibile, rassicuri gli interessati o perlomeno riduca il livello di allarme, utilizzando parole chiave facilmente rintracciabili sui motori di ricerca qualora venissero ricercate informazioni con tali modalità;

- le comunicazioni potrebbero non riguardare soltanto l'evento di Data Breach, ma anche le informazioni sull'andamento dello stesso nel tempo;
- assicurare forme di comunicazione oneste, concrete e trasparenti;
- fare riferimento al Team, al suo ruolo e al suo impegno;
- mettere in evidenza la storia, l'impegno di AIR CAMPANIA S.P.A. nell'assicurare l'attenzione al tema e le misure applicate;
- descrivere l'evento in modo facilmente comprensibile, quale impatto ha avuto sugli interessati (ovvero quali conseguenze possono presumibilmente avere la perdita di informazioni, la distruzione o la modifica, la comunicazione a terzi non autorizzati, la divulgazione, ecc.), come lo si sta affrontando, come è stato affrontato, specificare cosa AIR CAMPANIA S.P.A. sta facendo concretamente per proteggere i dati degli interessati;
- indicare quali misure tecniche sono state/saranno implementate per affrontare la violazione dei dati;
- indicare come e quando è stata coinvolta l'Autorità Garante della Protezione dei dati personali, o anche Agenzia di Cybersecurity Nazionale, Polizia Postale, Prefettura, etc..

8 Archiviazione

La documentazione richiamata in procedura è archiviata in formato elettronico e/o documentale a cura del Coordinatore Privacy per un periodo minimo di 5 anni, salvo diverse disposizioni normative.

9 Gestione non conformità

Qualora vengano riscontrate non conformità rispetto al processo descritto, si procederà al trattamento delle stesse secondo quanto previsto dalle procedure PGSI 03 "Gestione non conformità e reclami" e PGSI 04 "Azione correttive e miglioramento".