

COMUNE DI CALDIERO

Procedura data breach

Sommario

1_SCOPO DELLA PROCEDURA.....	3
2_DESTINATARI DELLA PROCEDURA.....	3
(Ambito soggettivo).....	3
3_AMBITO DI APPLICAZIONE	3
4_VIOLAZIONE DEI DATI	3
5_RUOLI COINVOLTI NELLA GESTIONE DEL <i>DATA BREACH</i>	3
6_FASI DEL PROCESSO DI <i>DATA BREACH</i>	4
Fase 1	4
Segnalazione incidente	4
Fase 2	4
2.1 Rilevazione e valutazione della violazione	4
2.2 Ricezione della segnalazione	4
2.3 Identificazione e classificazione della violazione	5
2.4 Identificazione delle cause	5
2.5 Valutazione dell’impatto della violazione e del rischio di danni agli interessati	5
2.5.1 Valutazione del rischio	5
Fase 3	6
Notifica all’Autorità di Controllo – GPDP	6
Fase 4	6
Comunicazione agli interessati.....	6
Fase 5	6
Registro violazioni	6
Fase 6	7
Azioni correttive.....	7

1_SCOPO DELLA PROCEDURA

Scopo della presente procedura è fornire istruzioni nel caso si verifichi un incidente sulla sicurezza che comporta una violazione dei dati personali (*data breach*).

La presente procedura:

- definisce i ruoli e le responsabilità organizzative per la gestione di un *data breach*;
- fornisce indicazioni pratiche e modalità operative per riconoscere e gestire situazioni relative a violazioni di dati al fine di minimizzarne l'impatto e prevenirne la reiterazione;
- fornisce la modulistica.

2_DESTINATARI DELLA PROCEDURA

(Ambito soggettivo)

La presente procedura ha come destinatari chiunque tratti dati personali all'interno o per conto dell'ente.

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata osservanza di quanto in essa previsto potrà comportare, rispettivamente a carico dei dipendenti, collaboratori e fornitori l'adozione di provvedimenti disciplinari, ovvero giusta causa di risoluzione dei contratti in essere.

3_AMBITO DI APPLICAZIONE

La presente procedura si applica in tutti i casi in cui si verifichi un incidente sulla sicurezza ed in particolare quando l'incidente comporta il rischio di una violazione dei dati.

4_VIOLAZIONE DEI DATI

(*data breach*)

Per violazione dei dati si deve intendere il rischio di perdita della:

- a) riservatezza dei dati
- b) integrità dei dati
- c) disponibilità dei dati

Tipo violazione	Specifica
Violazione della riservatezza dei dati	Accesso o trattamento non autorizzato o illecito Divulgazione non autorizzata
Violazione dell'integrità dei dati	Modifica non autorizzata o accidentale
Violazione della disponibilità dei dati	Perdita o distruzione accidentale o illegale Indisponibilità temporanea o prolungata

5_RUOLI COINVOLTI NELLA GESTIONE DEL DATA BREACH

Sono coinvolti nella gestione di un *data breach*:

- il Soggetto che ha scoperto il *data breach*;
- Il Preposto al trattamento dei dati oggetto di violazione;
- il Referente *privacy*;
- il Responsabile Transizione digitale/l'Amministratore di sistema/il Responsabile CED;
- il Responsabile della protezione dati (RPD/DPO);

6_FASI DEL PROCESSO DI DATA BREACH

Le fasi di gestione di un *data breach* sono le seguenti:

1	Analisi preliminare ed invio segnalazione
2	Gestione (contenimento del danno) e valutazione della gravità dell'evento
3	Notifica all'Autorità di controllo (Garante Protezione Dati Personali – GPDP)
4	Comunicazione agli interessati (ove necessario) e raccolta riscontro di avvenuta comunicazione
5	Inserimento nel registro delle violazioni
6	Azioni correttive specifiche e per analogia

Fase 1

Segnalazione incidente

Obiettivo della fase

Portare a conoscenza del (potenziale) *data breach* i soggetti competenti ad assumere le decisioni conseguenti nel più breve tempo possibile

Fase	Soggetti coinvolti	Azioni	Tempi	Modello
1	Chiunque venga a conoscenza di un (anche potenziale) <i>data breach</i>	Informazione al Referente <i>privacy</i> .	Tempestivo Il prima possibile.	All_1
	Referente <i>privacy</i>	Verifica preliminare dell'incidente finalizzata a verificare se si tratta di un " <i>falso positivo</i> " o di un vero <i>data breach</i> ; E' possibile il coinvolgimento del Responsabile dei sistemi informatici e/o amministratore di sistema.	Tempestivo Il prima possibile	
	Referente <i>privacy</i>	In caso di riscontro dell'esistenza di un <i>data breach</i> invio della segnalazione a: - RTD; - RPD/ DPO; - Responsabile sistemi informatici/Amministratore di sistema.	Tempestivo Il prima possibile.	

Fase 2

2.1 Rilevazione e valutazione della violazione

Obiettivo della fase

Valutare la gravità del *data breach* e conseguentemente se:

- non vi è alcun pericolo o danno per gli interessati;
- se il *data breach* deve essere notificato al GPDP;
- se il *data breach* deve essere comunicato agli interessati.

Fase	Soggetti coinvolti	Azioni	Tempi	Modello
2	- Referente <i>privacy</i> - Responsabile CED (laddove esistente) - RTD (Responsabile Transizione Digitale) - RPD/DPO (Responsabile Protezione Dati) - Dirigente/P.O Preposto al trattamento dei dati oggetto di violazione	- Ricezione della segnalazione. - Identificazione della violazione. - Classificazione della tipologia di violazione. - Identificazione delle cause. - Individuazione dei potenziali danni - Valutazione dell'impatto (gravità). - Decisioni conseguenti alla valutazione dell'impatto (gravità): - notifica Garante; - comunicazione interessati; - azioni correttive.	Il prima possibile e comunque entro 48 ore dalla segnalazione.	-

2.2 Ricezione della segnalazione

Ricevuta la segnalazione da parte del Referente *privacy* per l'ente viene convocata una riunione, anche da remoto, fra:

- Referente *privacy* per l'Ente;
- RTD (Responsabile Transizione Digitale);

- Responsabile sistemi informativi/Amministratore di sistema;
- RPD/DPO (Responsabile Protezione Dati).

2.3 Identificazione e classificazione della violazione

I soggetti coinvolti, anche con sopralluoghi ed acquisizione di informazioni:

- identificano con precisione la violazione;
- classificano la violazione in: **(i)** violazione della riservatezza dei dati; **(ii)** violazione dell'integrità dei dati; **(iii)** violazione della disponibilità dei dati.

La violazione può avere anche una classificazione plurima.

2.4 Identificazione delle cause

I soggetti coinvolti identificano le possibili cause della violazione.

2.5 Valutazione dell'impatto della violazione e del rischio di danni agli interessati

Potenziali danni e condizioni che vanno valutati ai fini della valutazione del rischio

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'Interessato a cui si riferiscono i dati, a causa della violazione dei dati personali:

- discriminazioni;
- furto o usurpazione d'identità;
- perdite finanziarie;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- decifrazione non autorizzata della pseudonimizzazione;
- danno economico o sociale significativo;
- privazione o limitazione di diritti o libertà;
- impedito controllo sui dati personali all'interessato;
- danni fisici, materiali o immateriali alle persone fisiche.

Dovranno inoltre essere valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

- che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- che si tratti di dati di persone fisiche vulnerabili, in particolare minori;
- che il trattamento riguardi una notevole quantità di Dati Personali;
- che il trattamento riguardi un vasto numero di Interessati.

2.5.1 Valutazione del rischio

Il rischio è calcolato mediante la seguente formula:

Rischio = probabilità di accadimento (del danno) X impatto

PROBABILITÀ DI ACCADIMENTO DEL DANNO	IMPATTO			
	Basso	Medio	Alto	Altissimo
Basso	1	2	3	4
Medio	2	4	6	8
Alto	3	6	9	12
Altissimo	4	8	12	16

La **probabilità di accadimento del danno** è valutata in base ai seguenti parametri

Parametro	Declinazione	Valutazione	
Molto improbabile	Il danno potrebbe dipendere da un concatenamento di eventi indipendenti; secondo gli addetti è impossibile il suo verificarsi oppure non è mai accaduto un danno simile	Basso	1
Poco probabile	Il danno potrebbe dipendere da condizioni sfavorevoli; eventi accaduti raramente	Medio	2
Probabile	Il danno potrebbe dipendere da condizioni non del tutto connesse alla situazione ma	Alto	3

	possibili; eventi già riscontrati in letteratura		
Molto probabile	Il danno potrebbe dipendere da condizioni connesse alla situazione; eventi già accaduti	Altissimo	4

L'impatto è valutato in base ai seguenti parametri

Basso	I soggetti interessati non vengono colpiti o subirebbero disagi minimi, superabili senza alcun problema (tempo necessario per reinserire le informazioni, fastidio, irritazione etc.)
Medio	I soggetti interessati subiscono disagi risolvibili con qualche difficoltà (costi extra, negazione accesso a servizi aziendali, timori, difficoltà di comprensione, stress, indisposizione fisica, etc.)
Alto	I soggetti interessati subiscono notevoli disagi risolvibili con serie difficoltà (appropriazione indebita di fondi, inserimento nella <i>black list</i> dei cattivi pagatori da parte delle banche, danni a proprietà, perdita dell'impiego, citazione a comparire, peggioramento dello stato di salute, discriminazioni etc.).
Altissimo	I soggetti interessati subiscono notevoli conseguenze, perfino irreversibili, e impossibili da risolvere (difficoltà finanziarie quali ingenti debiti, impossibilità a lavorare, problemi fisici o psicologici a lungo termine, morte, etc.) .

Fase 3

Notifica all'Autorità di Controllo – GPDP

Obiettivo della fase

Fornire l'informazione al GPDP e ricevere le eventuali indicazioni del GPDP

	Soggetti coinvolti	Azioni	Tempi	Modello
3	<ul style="list-style-type: none"> - Referente <i>privacy</i>; - RPD/DPO (Responsabile Protezione Dati); - RTD. 	<ul style="list-style-type: none"> - Notifica <i>data breach</i> al GPDP; - Ricezione indicazioni del GPDP. 	Nel più breve tempo possibile e comunque entro 72 dal momento della segnalazione (in caso di notifica al GPDP oltre le 72 ore va data adeguata motivazione del ritardo).	Procedura telematica GPDP

Fase 4

Comunicazione agli interessati

Obiettivo della fase

Comunicare agli interessati l'avvenuto *data breach* e gli eventuali pericoli per i dati che li riguardano.

Fase	Soggetti coinvolti	Azioni	Tempi	Modello
4	<ul style="list-style-type: none"> - Referente <i>privacy</i>; - RPD/DPO (Responsabile Protezione Dati); - RTD. 	<ul style="list-style-type: none"> - Comunicazione avvenuto <i>data breach</i> agli interessati 	Senza giustificato ritardo.	-

Fase 5

Registro violazioni

Obiettivo della fase

Documentare l'avvenuta violazione dei dati.

Fase	Soggetti coinvolti	Azioni	Tempi	Modello
5	<ul style="list-style-type: none"> - Referente <i>privacy</i>; - RPD/DPO (Responsabile Protezione Dati); 	<ul style="list-style-type: none"> - Registrazione della violazione (<i>data breach</i>) nel registro delle violazioni; - Registrazione eventuali comunicazione del GPDP; - Invio report della violazione al RTD; - Conservazione del Registro. 		All_2

Fase 6

Azioni correttive

Obiettivo della fase

Individuare ed adottare misure correttive ai fini della riduzione delle probabilità di verifica di altro *data breach* e dei possibili danni derivanti dal *data breach*.

Fase	Soggetti coinvolti	Azioni	Tempi	Modello
6	<ul style="list-style-type: none">- RTD;- Referente <i>privacy</i>;- RPD/DPO (Responsabile Protezione Dati);	<ul style="list-style-type: none">- Individuazione azioni correttive per ridurre la probabilità di accadimento e gli eventuali danno conseguenti alla violazione;- Attuazione delle azioni correttive.	Da definire	-

