Allegato B)

UNIONE DI COMUNI VERONA EST

(Provincia di VERONA)

PROCEDURA IN CASO DI DATA BREACH

Linee operative

Approvate con deliberazione di Giunta Unione n._____del_____

Allegato B)

Sommario

Allegato B)

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 coloro che trattino 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)

Allegato B)

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) *data breach*	Informazione al Referente privacy	Tempestivo Il prima possibile	All_1
	Referente privacy	Verifica preliminare dell'incidente finalizzata a verificare se si tratta di un "*falso positivo*" o di un vero *data breach* E' possibile il coinvolgimento del Responsabile dei sistemi informatici e/o amministratore di sistema	Tempestivo Il prima possibile	
	Referente privacy	In caso di riscontro dell'esistenza di un *data breach* 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:

a) non vi è alcun pericolo o danno per gli interessati;
b) se il data breach deve essere notificato al Garante per la Protezione dei Dati Personali;
c) se il data breach deve essere comunicato agli interessati.

Fase	Soggetti coinvolti	Azioni	Tempi	Modello

2	- Referente privacy
	- 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:

a) identificano con precisione la violazione;

b) 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:

a) discriminazioni
b) furto o usurpazione d'identità
c) perdite finanziarie
d) pregiudizio alla reputazione
e) perdita di riservatezza dei dati personali protetti da segreto professionale
f) decifratura non autorizzata della pseudonimizzazione
g) danno economico o sociale significativo
h) privazione o limitazione di diritti o libertà
i) impedito controllo sui dati personali all'interessato
j) danni fisici, materiali o immateriali alle persone fisiche.

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

(i) 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;

(ii) 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;

(iii) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

(iv) che il trattamento riguardi una notevole quantità di Dati Personali;

(v) 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*

	IMPATTO			
PROBABILITÀ DI ACCADIMENTO DEL DANNO	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

Allegato B)

Probabile	Il danno potrebbe dipendere da condizioni non del tutto connesse alla situazione ma possibili; eventi già riscontrati in letteratura	Alto	3
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 black list 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	- Referente privacy - RPD/DPO (Responsabile Protezione Dati) - RTD	- Notifica data breach 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	- Referente privacy - RPD/DPO (Responsabile Protezione Dati) - RTD	- Comunicazione avvenuto data breach agli interessati	Senza giustificato ritardo	-

Fase 5

Registro violazioni

Obiettivo della fase

Documentare l'avventa violazione dei dati

Fase	Soggetti coinvolti	Azioni	Tempi	Modello
5	- Referente privacy - RPD/DPO (Responsabile Protezione Dati)	- Registrazione della violazione (data breach) nel registro delle violazioni - Registrazione eventuali comunicazione del GPDP - Invio report della violazione al RTD - Conservazione del registro		All_2

Allegato B)

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	- RTD - Referente privacy - RPD/DPO (Responsabile Protezione Dati)	- Individuazione azioni correttive per ridurre la probabilità di accadimento e gli eventuali danno conseguenti alla violazione - Attuazione delle azioni correttive	Da definire	-

Allegato B)

ALLEGATO 1

MODELLO SEGNALAZIONE INCIDENTE SICUREZZA / VIOLAZIONE DATI

1_SEGNALANTE

Nome	
Cognome	
Area / settore / ufficio	
Superiore di riferimento	

2_INFORMAZIONI SULL'INCIDENTE

Data e ora in cui si è venuti a conoscenza dell'incidente[1]	
Luogo dell'incidente	
Descrizione dell'incidente	

3_DISPOSITIVO OGGETTO DELLA VIOLAZIONE

Tipologia di dispositivi	**Descrizione sintetica dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione**
Computer	
Server	
Storage	
Rete	
Dispositivo mobile	
File o parte di un file	
Strumento di backup	
Documento cartaceo	
Altro	

4_TIPO DI INCIDENTE [2]

Violazione della riservatezza *Accesso o trattamento non autorizzato o illecito* *Divulgazione non autorizzata*	
Violazione della integrità *Modifica non autorizzata o accidentale*	
Violazione della disponibilità *Perdita o distruzione accidentale o illegale* *Indisponibilità temporanea o prolungata*	

5_TIPO DI VIOLAZIONE [3]

Lettura Presumibilmente è stato effettuato un accesso ai dati ma i dati non sono stati copiati	
Copia *I dati sono ancora presenti sui sistemi del titolare ma copiati dall'autore della violazione)*	
Alterazione *I dati sono presenti sui sistemi del titolare ma sono stati alterati)*	
Cancellazione	

[1] Se non si conosce precisamente l'ora indicare il tempo approssimativo: (**i**) il giorno; (**ii**) tra …. e…; (**iii**) tempo non determinato; (**iv**) ancora in corso.
[2] Indicare una o più tipologie di violazione
[3] Indicare uno o più tipi di violazione

Allegato B)

I dati non sono più sui sistemi del titolare e non sono neppure in possesso dell'autore della violazione)	
Furto I *dati non sono più sui sistemi del titolare ma sono presumibilmente in possesso dell'autore della violazione)*	
Indisponibilità I *dati sono presenti sui sistemi del titolare ma non sono disponibili per un certo periodo di tempo)*	
Altro	

6_INFORMAZIONI SUL TRATTAMENTO OGGETTO DELL'INCIDENTE E SUI DATI TRATTATI

Trattamento[4]	
Categoria di dati personali trattati [5]	
Specifica dei dati trattati ed oggetto dell'incidente[6]	

7_INFORMAZIONI SUGLI INTERESSATI DALL'INCIDENTE

Categoria di interessati[7]	
Numero di interessati coinvolti	
Potenziali conseguenze della violazione	
Descrizione dell'impatto della violazione	

8_AZIONI INTRAPRESE

Indicare le azioni intraprese dopo l'avvenuta scoperta dell'incidente	

[4] Indicare il trattamento o i trattamenti oggetto dell'incidente possibilmente facendo riferimento al registro dei trattamenti.
[5] Indicare la tipologia (anche più di una di dati trattati: (a) dati comuni; (b) dati particolari; (c) dati giudiziari.

[6] Specificare nel dettaglio di che dati si tratta: Dati anagrafici/codice fiscale □ Dati di accesso e di identificazione (es. username, password, altro) □ Dati relativi a minori □ Dati relativi a altri soggetti vulnerabili □ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati □ Dati economico finanziari (es. numero carta di credito) □ Dati genetici □ Dati relativi alla salute □ Dati giudiziari 17 □ Dati biometrici

[7] Indicare una o più categorie di interessati: [ ] Dipendenti; [ ] collaboratori; [ ]professionisti; [ ]Fornitori; [ ] Cittadini / Consumatori [ ] Altro (specificare).

Allegato B)

ALLEGATO 2

REGISTRO DATA BREACH

Numero Violazione	Data Violazione	Natura della Violazione	Categoria di Interessati	Categoria di dati personali coinvolti	Numero approssimativo di registrazioni dati personali	Conseguenze della Violazione	Contromisure adottate	Notifica Autorità Garante Privacy (S/N)	Comunicazione ai soggetti interessati (S/N)