COMUNE DI SAN MICHELE DI GANZARIA
Via Roma, 82/84 - Cap. 95040, cap 95040– San Michele di Ganzaria (CT)
Codice Fiscale 82002180873 Partita IVA 01180410878 – Tel (+39) 0933 971011
Mail: segreteria@comune.sanmicheleganzaria.ct.it
PEC: prot.gen@pec.comune.sanmicheleganzaria.ct.it

# # #

Playbook per la gestione delle violazioni dei dati personali (data breach)

# # #

1. Titolo e Versione

- **Oggetto:** *Piano di Risposta per la Gestione delle Violazioni della Sicurezza dei Dati (Data Breach).*
- **Versione:** 1.0 del 04/02/2026 – approvato dall'amministrazione con delibera GC n 28 del 20/03/2026.

2. Descrizione

Il presente playbook descrive le azioni coordinate da attuare in caso di **violazioni concrete, potenziali o sospette** di dati personali.
Il documento mira a proteggere i diritti e le libertà degli interessati, prevenire danni economici all'Ente e garantire il rispetto degli obblighi di notifica all'Autorità Garante e di comunicazione agli interessati previsti dal GDPR.
La procedura si applica a tutti i dati personali trattati dal Titolare, in qualsiasi formato (cartaceo o digitale).

3. Condizioni di Attivazione

Le procedure vengono attivate al verificarsi di un **evento di Data Breach**, definito come una *violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione o accesso non autorizzato a dati personali*.

Logiche di rilevamento ed esempi di attivazione:

- **Rilevamento manuale:** Segnalazione da parte di dipendenti, collaboratori o responsabili esterni che vengono a conoscenza di un incidente.
- **Esempi di eventi scatenanti:**
  - Smarrimento o furto di laptop, dispositivi informatici o documenti cartacei.
  - Attacchi informatici (virus, pirateria, accesso abusivo a sistemi protetti).
  - Errori umani, come l'invio di e-mail contenenti dati personali a destinatari errati.
  - Infedeltà del dipendente o divulgazione non autorizzata a terzi.
  - Indisponibilità definitiva dei dati dovuta a distruzione non autorizzata.

4. Attività

Il processo si articola in sette fasi sequenziali:

- **Fase 1: Rilevamento e Indagine Preliminare**
  - Chiunque rilevi la violazione deve informare immediatamente il Titolare, l'RPD e la persona designata.
  - Acquisizione delle informazioni chiave (cosa, quando, chi) e compilazione della **Scheda di Rilevamento** (Allegato A).
  - Annotazione dell'evento nel **Registro dei Data Breach**.
  - **Importante:** Non cancellare file o prove digitali prima della fine degli accertamenti.
- **Fase 2: Contenimento della Violazione**
  - Attuazione di azioni per rimuovere le cause e limitare i danni (es. isolamento rete, cambio password, ripristino da backup).
  - Identificazione delle misure per evitare la reiterazione dell'evento.
- **Fase 3: Valutazione del Rischio**
  - Stima della probabilità e della gravità del rischio per i diritti delle persone fisiche utilizzando i criteri dell'Allegato B (natura dei dati, volume, facilità di identificazione).
  - Determinazione dell'obbligo di notifica in base alla probabilità del rischio.
- **Fase 4: Notifica all'Autorità Garante**
  - Se viene valutata la presenza di un rischio, il Titolare effettua la notifica al Garante senza ingiustificato ritardo, al massimo **entro 72 ore** dalla conoscenza dell'evento.
  - In caso di informazioni incomplete, si procede con una notifica preliminare seguita da una integrativa.
- **Fase 5: Comunicazione agli Interessati**
  - Se il **rischio è elevato**, la violazione deve essere comunicata direttamente agli interessati in modo chiaro e tempestivo.

- La comunicazione deve includere la natura della violazione, i dati di contatto dell'RPD e le misure adottate.

- **Fase 6: Documentazione della Violazione**
  - Archiviazione di tutta la documentazione (Allegati A e B) e aggiornamento costante del Registro dei Data Breach, a disposizione dell'Autorità.
- **Fase 7: Verifica e Revisione**
  - Analisi post-evento per individuare cause profonde e migliorare le misure preventive future.

---

5. Ruoli e Responsabilità (Matrice RASCI)

Per la corretta attuazione delle attività, si definisce la seguente matrice di responsabilità:

Attività / Fase	Titolare del Trattamento (Sindaco)	Persona Designata	RPD (DPO)	Amministratore di Sistema Funzionari/Dirigenti/ Responsabile d'area	Dipendenti autorizzati al trattamento
Rilevamento e Segnalazione	**A**	**S**	**I/C**	**R/I**	**R**
Indagine Preliminare	**A**	**R**	**I/C**	**I/S**	**S**
Contenimento	**A**	**S**	**C**	**R**	**S**
Valutazione del Rischio	**A**	**S**	**C**	**R**	**S**
Notifica al Garante	**R/A**	**S**	**I/C**	**R**	**-**
Comunicazione agli Interessati	**A**	**S**	**C**	**R**	**I**
Tenuta Registro e Documentazione	**A**	**R**	**C**	**I**	**S**
Revisione Post-Incidente	**A**	**S**	**C**	**R**	**I**

Note sui ruoli:

- **Titolare (Accountable):** Ha la responsabilità finale di ogni adempimento e decisione.
- **Persona Designata (Responsible):** Gestisce operativamente la procedura, compila le schede e aggiorna il registro.

  - **Designati data breach:** Dirigente Area Amm / Saitta Antonio

- **RPD (Consulted):** Fornisce consulenza specialistica e supervisiona l'intero processo.
- **Amministratore di Sistema (Support/Responsible):** Supporta le indagini tecniche e agisce per il contenimento sui sistemi informatici.
- **Dipendenti (Responsible for detection):** Effettuano la segnalazione immediata di qualsiasi anomalia.

6. Rinvio alle Istruzioni operative per il personale

Salvo quanto previsto nel presente playbook, rimane applicabile quanto già previsto nel ***Piano di Risposta per la Gestione delle Violazioni della Sicurezza dei Dati (Data Breach)*** già approvato dall'amministrazione con delibera G.M. n. 122 del 24.12.2019.

Note:

- *La mancata conformità a queste regole può comportare provvedimenti disciplinari per i dipendenti o la risoluzione dei contratti per le terze parti.*
- ***Accountability:** Tutte le misure devono essere documentate per dimostrare che il trattamento è effettuato conformemente al Regolamento.*
- ***Segretezza:** Il Responsabile e il personale autorizzato sono vincolati all'obbligo di **riservatezza** e non possono trasferire dati extra UE senza autorizzazione.*

Allegato A)

SCHEDA DI RILEVAMENTO DI UNA

VIOLAZIONE DELLA SICUREZZA DEI DATI PERSONALI

(DATA BREACH)

1	**Data** dell' evento	☐ Il _____ ☐ Dal _____ (la violazione è ancora in corso) ☐ Dal _____ al _____ ☐ In un tempo non ancora determinato
2	**data e ora** in cui si è venuti a **conoscenza** dell'evento	Data:_____ Ora:_____
3	data e ora del **termine di scadenza** della **notifica** al Garante (*calcolare **72 ore** dal momento in cui si è avuta conoscenza*)	Data:_____ Ora:_____
4	**Data, ora e modalità** in cui è stato **informato il RPD**	Data:_____ Ora:_____ Modalità: _____
5	**Data, ora e modalità** in cui è stato **informato il Titolare**	Data:_____ Ora:_____ Modalità: _____

6	**Indicare se è stata data comunicazione del Data Breach ad altri soggetti** *(ad esempio, ai Contitolari, ad altri Titolari, a Responsabili esterni)*	☐ **NO** ☐ **Si - indicare** Data:_____ Ora:_____ Modalità: _____

7	**fonte** attraverso la quale si è avuta conoscenza dell'evento *(eventuali **generalità complete** e **dati di contatto** (telefono, mail) della persona che per prima ha rilevato la violazione - in caso di soggetti esterni/società indicare la denominazione e la ragione sociale)*	
8	**Luogo della violazione** *(indicare l'ufficio o gli uffici coinvolti)*	
8.1	**la violazione concerne**	☐ trattamenti per finalità amministrative ☐ trattamenti per finalità di Polizia ex D.Lg.s 2018 n.51

9	**Dispositivi oggetto del Data Breach**	☐ computer ☐ server ☐ rete ☐ portatile ☐ tablet, smatphone ☐ chiavette usb, dispositivi di archiviazione esterne ☐ file o parte di un file ☐ account posta elettronica ☐ account PEC ☐ piattaforme on line ☐ strumento di back up ☐ documento cartaceo
10	**Se è coinvolto uno strumento di back up indicare quando è stato fatto l'ultimo back up**	☐ ultimo back up effettuato In data _____
11	**Se un laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?**	☐ ultima sincronizzazione effettuata In data _____

12	**Soggetti interni il cui trattamento è coinvolto dall'evento**	
13	**Ulteriori soggetti esterno, il cui trattamento è coinvolto dall'evento** *(in caso di società indicare la ragione sociale - Indicare il **ruolo** svolto: contitolare, responsabile, altro titolare esterno)*	Denominazione:_____ C.f. / P.Iva: _____ Ruolo: ☐ Contitolare ☐ Responsabile esterno ☐ altro titolare per conto del quale l'ente tratta dati
14	**natura della violazione** dei dati personali *(descrivere il tipo di violazione, specificando le modalità ed eventuali nomi di soggetti coinvolti in maniera lecita o illecita, volontaria o involontaria o accidentale, denominazione dell'archivio o della banca dati coinvolto)*	☐ Perdita di confidenzialità ☐ Perdita di integrità ☐ Perdita di disponibilità

		☐ attività lecite ☐ attività illecite ☐ Attività volontarie ☐ Attività involontarie ☐ Attività accidentali
		☐ eventuali nomi di soggetti coinvolti: _____ ☐ Archivio o banca dati coinvolta: _____ ☐ Descrizione delle modalità con le quali si è verificato l'evento: _____
15	**Causa della violazione**	☐ Azione intenzionale interna ☐ Azione accidentale interna ☐ Azione intenzionale esterna ☐ Azione accidentale esterna ☐ Sconosciuta ☐ Altro (specificare): _____

16	**categorie di dati** coinvolti dall'evento	☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...) ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…) ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…) ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione ☐ Dati di profilazione ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…) ☐ Dati di localizzazione ☐ Dati che rivelino l'origine razziale o etnica ☐ Dati che rivelino opinioni politiche ☐ Dati che rivelino convinzioni religiose o filosofiche ☐ Dati che rivelino l'appartenenza sindacale ☐ Dati relativi alla vita sessuale o all'orientamento sessuale

17	**Volume dei dati personali coinvolti** *(stimare anche in modo approssimativo la quantità dei dati personali coinvolti dall'evento)*	☐ N._____ di dati coinvolti ☐ Circa n. _____ di dati coinvolti ☐ Un numero ancora sconosciuto di dati coinvolti
18	**categorie di interessati** coinvolti dall'evento	☐ Dipendenti ☐ Consulenti ☐ Utenti ☐ Contraenti ☐ Abbonati ☐ Clienti (attuali o potenziali) ☐ Associati, soci, aderenti, simpatizzanti, sostenitori ☐ Soggetti che ricoprono cariche sociali ☐ Beneficiari o assistiti ☐ Pazienti ☐ Minori ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) ☐ Categorie ancora non determinate

		☐ Altro (specificare) _____
19	**numero** di **interessati** (*anche approssimativo*)	☐ N._____ interessati ☐ Circa n. _____interessati ☐ Un numero (ancora) sconosciuto di interessati
20	**Descrizione dell'incidente di sicurezza alla base della violazione**	

21	**categorie** di **registrazioni** dei dati personali coinvolti	
22	**numero** approssimativo di **registrazioni** dei dati personali convolte	
23	Descrizione dei sistemi e delle infrastrutture IT coinvolti, con indicazione della loro ubicazione.	
24	Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti	

25	Descrizione delle probabili **conseguenze** della violazione	**In caso di perdita di confidenzialità:** ☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati ☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito ☐ Altro (specificare): _____
		In caso di perdita di integrità: ☐ I dati sono stati modificati e resi inconsistenti ☐ I dati sono stati modificati mantenendo la consistenza ☐ Altro (specificare):_____
		In caso di perdita di disponibilità: ☐ Mancato accesso a servizi ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi ☐ Altro (specificare): _____
		Ulteriori considerazioni sulle possibili conseguenze:_____

26	**Potenziali effetti negativi** per gli interessati	☐ Perdita del controllo dei dati personali ☐ Limitazione dei diritti ☐ Discriminazione ☐ Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Decifratura non autorizzata della pseudonimizzazione ☐ Pregiudizio alla reputazione ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale ☐ Conoscenza da parte di terzi non autorizzati ☐ Qualsiasi altro danno economico o sociale significativo (specificare)
27	Modalità di esposizione al rischio	☐ lettura (presumibilmente i dati non sono stati copiati), ☐ copia (i dati sono ancora presenti sui sistemi del titolare), ☐ alterazione (i dati sono presenti sui sistemi ma sono stati alterati), ☐ cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), ☐ furto (i dati non sono più sui sistemi del titolare e li ha l'autore della
28	Ruolo del Titolare e natura dell'attività svolta	violazione) trattamenti effettuati per ☐ adempiere un obbligo legale o nell'esercizio di pubblici poteri ☐ erogazione di servizi pubblici essenziali ☐ erogazione di servizi facoltativi non essenziali

29	La violazione può avere conseguenze negative in uno dei seguenti ambiti ?	☐ gestione dei servizi resi all'utenza ☐ ricerca ☐ finanziario, patrimoniale, contabile ☐ giudiziario ☐ responsabilità ☐ reputazione - immagine
30	La violazione concerne informazioni che possono essere utilizzate per commettere furti d'identità ?	☐ dati di accesso e di identificazione ☐ codice fiscale ☐ copie di carta d'identità ☐ passaporto ☐ carte di credito
31	La violazione coinvolge informazioni relative a performance lavorative che potrebbero causare danni significativi alle persone	☐ salario o stipendio ☐ stato di famiglia ☐ sanzioni disciplinari ☐ altro _____

32	Gli interessati rischiano di essere privati del controllo sui dati personali che li riguardano?	☐ Si ☐ No
33	Facilità con cui un soggetto che può accedere a dati personali compromessi riesce ad identificare persone fisiche specifiche anche abbinando i dati con altre informazioni	☐ Molto facile (non occorre una ricerca speciale per risalire all'identità) ☐ difficile, ma non impossibile in presenza di certe condizioni ☐ estremamente difficile
34	E' **PROBABILE** che vi sia un **RISCHIO** per i diritti e le libertà delle persone fisiche? (***MOTIVARE*** *adeguatamente*)	☐ Si ☐ No Motivazione:
35	**Misure** tecniche e organizzative adottate o di cui si propone l'adozione per porre **rimedio** alla violazione dei dati e **ridurne** gli effetti negativi per gli interessati. *(ad esempio: La pseudonimizzazione e la cifratura dei dati personali)*	
	Misure tecniche e organizzative adottate o di cui si propone l'adozione per **prevenire simili violazion**i future	
36	La violazione è suscettibile di presentare un **RISCHIO ELEVATO** per i diritti e le libertà delle persone fisiche ? (***MOTIVARE*** *adeguatamente)*	☐ Si ☐ No Motivazione:

37	**Classificazione della gravità della violazione e motivazioni:**	☐ Trascurabile ☐ Basso ☐ Medio ☐ Alto Motivazione:
38	**Prima della violazione** il titolare aveva 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 <u>incomprensibili</u>** a chiunque non sia autorizzato ad accedervi ? (ad es. cifratura)	☐ No ☐ Si, (specificare quali_____
39	Sono state **successivamente** adottate misure atte a **scongiurare il sopraggiungere** di un rischio elevato per i diritti e le libertà degli interessati ?	☐ No ☐ Si, (specificare quali_____
40	**La comunicazione** agli interessati richiederebbe **sforzi sproporzionati** (**MOTIVARE** adeguatamente)	☐ No ☐ Si, (specificare per quale motivo): _____
26	Indicare se la violazione è **collegata** con altre che riguardino il medesimo tipo di dati personali che siano stati violati nel medesimo modo e in un lasso di tempo relativamente breve.	
27	Indicare eventuali **altri documenti utili** per documentare l'evento	

Data _____ F.to Il designato per la procedura di data breach

_____

Data _____ Il Titolare - F.to Il Sindaco legale rappresentante

_____

Allegato B)

GRIGLIA PER STIMARE LA PROBABILITA' E LA GRAVITA' DEL RISCHIO CONNESSO AL DATA BREACH

ALLA LUCE DELLA SCHEDA DI RILEVAMENTO E DEGLI ALTRI ELEMENTI DI VALUTAZIONE ACQUISITI

CRITERI PER VALUTAZIONE LA PROBABILITA' LA GRAVITÀ DEL RISCHIO		**Motivazione**	
Fattori da considerare alla luce della Scheda allegato A)		**PROBABILITA'**	**GRAVITA'**
Tipo di violazione	violazione della riservatezza, della disponibilità dell'integrità in relazione a • tipo di dati • categorie di interessati. vi è contemporaneamente una combinazione di più violazioni o una loro reiterazione ?		
Natura e carattere sensibile dei dati personali violati	Qual è il grado di sensibilità dei dati coinvolti dati comuni categorie particolari di dati dati giudiziari penali		
Volume dei dati violati	Qual è il volume dei dati coinvolti ?		
Numero di persone fisiche interessate	Qual è il numero di interessati ?		
Facilità di identificazione delle persone fisiche anche abbinando i dati con altre informazioni	☐ Molto facile (non occorre una ricerca speciale per risalire all'identità) ☐ difficile, ma non impossibile in presenza di certe condizioni ☐ estremamente difficile		
Gravità delle conseguenze a seconda della natura dei dati coinvolti	Stimare i potenziali effetti negativi per gli interessati indicati nella scheda allegato A		
Caratteristiche particolari dell'interessato	la violazione riguarda dati riferiti a ☐ Minori ☐ Anziani ☐ Disabili ☐ o altre categorie di persone vulnerabili il rischio di danno è più elevato		
Caratteristiche particolari del Titolare del trattamento e natura dell'attività svolta	distinguere i trattamenti effettuati per adempiere un obbligo legale o nell'esercizio di pubblici poteri erogazione di servizi pubblici essenziali erogazione di servizi facoltativi non essenziali		
Giudizio finale sul Rischio		☐ **PROBABILE** ☐ **IMPROBABILE**	☐ **Trascurabile** ☐ **Basso** ☐ **Medio** ☐ **Alto**