



# 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.sanmichelediganzaria.ct.it](mailto:segreteria@comune.sanmichelediganzaria.ct.it)

PEC: [prot.gen@pec.comune.sanmichelediganzaria.ct.it](mailto:prot.gen@pec.comune.sanmichelediganzaria.ct.it)

###

## Playbook sulle Istruzioni operative per il personale autorizzato al trattamento dei dati personali

###

### 1. Titolo e Versione

- **Titolo:** *Istruzioni operative al personale autorizzato al trattamento dei dati personali*
- **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 procedure operative standard che tutto il personale autorizzato deve seguire per garantire la **riservatezza, l'integrità e la disponibilità** dei dati personali trattati dall'Ente.

Copre la gestione dei documenti cartacei, la sicurezza dei dispositivi elettronici, l'uso della posta elettronica e la gestione delle richieste degli interessati.

### 3. Condizioni di Attivazione

Le procedure previste si attivano al verificarsi dei seguenti eventi:

- **Assegnazione o utilizzo di strumenti informatici:** Ogni volta che un dipendente accede a PC, mail o account istituzionali.
- **Ricezione di comunicazioni:** All'arrivo di mail o PEC da parte di cittadini o terzi.
- **Rilevamento di anomalie:** Segnalazioni dell'antivirus, ricezione di file sospetti o malfunzionamenti dei dispositivi.
- **Richiesta di esercizio dei diritti:** Quando un cittadino richiede l'accesso, la rettifica o la cancellazione dei propri dati.
- **Procedure di pubblicazione:** Necessità di pubblicare atti sul sito web istituzionale o all'Albo Pretorio.
- **Sospetta violazione dei dati (Data Breach):** Rilevamento di accessi non autorizzati e/o perdita di dati e/o perdita della disponibilità dei dati.

**Logiche di rilevamento:** Monitoraggio costante dei sistemi di protezione (firewall, antivirus), controllo quotidiano della posta in entrata e vigilanza fisica sui locali e sui documenti.

### 4. Attività per Fase del Processo

#### Fase A: Configurazione e Sicurezza Preventiva

- **Gestione Password:** Creare password di almeno 8 caratteri alfanumerici, non riferibili al dipendente, e consegnarle in busta chiusa al Dirigente d'area che assicura la conservazione in cassaforte (o cassetto chiuso a chiave) con facoltà di delegare un responsabile dell'ufficio Anagrafe o della Polizia Municipale o dell'Economato provvisti di cassaforte.
  - Nel caso di assenza o impedimento del dipendente al quale è assegnato il PC, qualora sia necessario ed indispensabile accedere al PC per esigenze dell'ufficio, il Dirigente procederà a:
    - aprire la busta
    - autorizzare l'accesso temporaneo di un altro dipendente per esigenze dell'ufficio
    - redigere un verbale che indichi le ragioni che hanno reso necessario tale accesso
    - informare (anche telefonicamente) il dipendente al quale il PC è assegnato dell'avvenuta modifica della password per esigenze dell'ufficio.

Al suo rientro in servizio il dipendente al quale è assegnato il dispositivo procederà a modificare la password ripetendo la procedura di annotazione in busta chiusa e consegna sopra descritta.

- La **password è personale**, non deve essere condivisa né trascritta su fogli disponibili a terzi e deve esserne assicurata la segretezza.
- **Protezione Postazione:** Collocare i monitor in modo che non siano visibili a non autorizzati e attivare lo screen saver automatico dopo 3 minuti di inattività.
- **Manutenzione:** Assicurarsi che antivirus e sistema operativo siano aggiornati almeno settimanalmente.

#### Fase B: Operatività Quotidiana

- **Gestione Documentale:** Conservare i fascicoli in armadi chiusi a chiave; distruggere i documenti cartacei inutili tramite distruggidocumenti meccanici.
- **Comunicazioni Elettroniche:** Verificare sempre l'indirizzo del destinatario; criptare i file contenenti categorie particolari di dati prima dell'invio. In caso di invio di mail o pec a molti destinatari, specialmente se privati, è necessario inserire gli indirizzi dei co-destinatari nel **campo Ccn** in modo da non consentire di visualizzare gli indirizzi degli altro co-destinatari, salvo che ciò sia richiesto da finalità istituzionali specifiche.
- **Social media:** Non è consentito comunicare o diffondere dati personali o documenti o atti dell'ufficio attraverso i social network (Facebook, WhatsApp, Instagram, Twitter, LinkedIn, ecc.).
- **Finalità:** I dati raccolti non verranno trattati per finalità diverse e incompatibili con quelle per le quali sono stati raccolti.
- **Necessità, Pertinenza e Proporzionalità:** Possono essere raccolti solo i dati necessari, pertinenti e proporzionati alle finalità perseguite dall'amministrazione nell'esercizio dei propri compiti istituzionali e nell'erogazione dei servizi resi.
- **Minimizzazione:** Raccogliere solo i dati strettamente necessari per le finalità perseguite e non effettuare copie non indispensabili.
- **Esattezza:** I moduli e le schede compilati dagli utenti o dal personale interno devono essere sempre controllati accuratamente verificando l'esattezza e correttezza dei dati inseriti. I dati errati, parziali o incompleti devono essere immediatamente corretti e aggiornati.
- **Trasparenza:** quando si raccolgono dati personali è necessario rendere sempre l'informativa prevista dall'art. 13 GDPR (prima di raccogliere i dati, se i dati vengono ottenuti direttamente dall'interessato) o dall'art. 14 GDPR (non oltre la prima comunicazione dei dati, se i dati vengono raccolti da terzi o da altre fonti).
- **Durata:** I dati non verranno trattati oltre i tempi previsti per il conseguimento delle finalità per le quali sono stati raccolti o ottenuti o oltre i tempi previsti dalle norme vigenti in relazione ai singoli procedimenti amministrativi.

#### Fase C: Gestione Eventi e Richieste

- **Risposta agli Interessati:** Riscontrare le richieste di esercizio dei diritti (accesso, rettifica, opposizione, limitazione, portabilità, ecc.) tempestivamente, al massimo **entro un mese**; in caso di proroga del termine, informare l'interessato.
- **Verifica Allegati Sospetti:** Non aprire file con estensioni eseguibili (.exe, .sys) o provenienti da mittenti sconosciuti; in caso di dubbio, contattare l'assistenza tecnica o il RPD.
- **Pubblicazione Atti:** Prima della pubblicazione online, oscurare i dati eccedenti e verificare l'esistenza di un obbligo normativo.

#### Fase D: Archiviazione e Chiusura

- **Back-up:** Effettuare il back-up sistematico dei dati su supporti esterni forniti dall'amministrazione, almeno ogni 8 giorni e annotare la data su un registro cartaceo. I supporti esterni utilizzati per il backup devono essere criptografati con una chiave di cifratura robusta e conservati in cassaforte o in cassette tenuti chiusi a chiave.
- **Cancellazione:** Svuotare il cestino del PC almeno ogni 15 giorni ed eliminare i documenti e i file al termine del periodo di conservazione previsto.

## 5. Ruoli e Responsabilità (Matrice RASCI)

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

Attività / Fase	Personale Autorizzato (Dipendenti)	Dirigente di Area	Designato Gestione Diritti	Designato Data Breach	Responsabile Protezione Dati (RPD)
Gestione quotidiana sicurezza PC/Password	R	A/I	-	-	C
Conservazione documenti cartacei	R	A/I	-	I	C
Predisposizione e firma Informativa ex artt.13 e 14	S	R/A	-	-	C
Resa delle Informativa agli interessati	R	A	-	-	-
Riscontro a istanze di accesso/rettifica	R	A/I	S	-	I/C
Rilevamento/Segnalazione Data Breach	R	A/I	-	I/S	I/C
Pubblicazione atti su sito web	R	A/I	-	-	C
Manutenzione sistemi e back-up	R	A/I	-	-	C

### Legenda RASCI:

- **R (Responsible):** Colui che esegue l'attività.
- **A (Accountable):** Colui che ha la responsabilità ultima e approva il lavoro.
- **S (Support):** Chi fornisce supporto per l'esecuzione:

▪ <b>Designati data breach:</b>	Dirigente Area Amm. / Saitta Antonio
▪ <b>Designato gestione diritti:</b>	Francesca Casciana

- **C (Consulted):** Chi deve essere consultato.
- **I (Informed):** Chi deve essere informato dei risultati.

## 6. Rinvio alle Istruzioni operative per il personale

Salvo quanto previsto nel presente playbook, rimane applicabile quanto già previsto nelle **Istruzioni operative per il personale autorizzato al trattamento dei dati personali** già approvate dall'amministrazione con delibera G.M. n. 14 del 29.1.2019, emendate il 24.12.2019, con delibera G.M. n. 122 del 24.12.2019, emendate il 5.4.2022 con delibera G.M. n. 39 del 17.05.2022, con ultimo aggiornamento del 10 giugno 2025

*Nota: La mancata conformità a queste regole può comportare provvedimenti disciplinari per i dipendenti o la risoluzione dei contratti per le terze parti.*