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 dei Rapporti con i Responsabili Esterni del Trattamento e la definizione dei ruoli con i Contitolari

# # #

1.Titolo e Versione

- **Oggetto:** *Procedure per la selezione, contrattualizzazione e monitoraggio dei Responsabili Esterni del Trattamento ai sensi dell'art.28 GDPR e per la definizione dei ruoli del trattamento con i Contitolari ai sensi dell'art. 26 GDPR.*
- **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 linee guida operative per

- garantire che i trattamenti effettuati per conto del **Titolare del trattamento,** da altri soggetti esterni, che rivestono il ruolo di **"Responsabili",** siano conformi al Regolamento UE 679/2016 (GDPR). Il documento descrive il processo di verifica delle garanzie fornite dai responsabili, la formalizzazione dei rapporti contrattuali e le attività di monitoraggio continuo e gestione delle criticità;
- assicurare una corretta definizione dei ruoli del trattamento effettuato in situazione di "contitolarità" con altri enti in conformità a quanto prevede l'art. 26 GDPR.

3.Condizioni di Attivazione

L'esecuzione delle procedure previste è determinata dai seguenti eventi:

- **Esigenza di esternalizzare** un trattamento di dati personali e conferire un nuovo incarico ad un soggetto estraneo all'ente.
- **Indizione di gare**, manifestazioni d'interesse o procedure di aggiudicazione appalti.
- **Scadenza periodica** dei termini per il monitoraggio della conformità o imminente scadenza contrattuale.
- **Rilevazione di anomalie**, come la mancata sottoscrizione dell'accordo Art. 28 o istruzioni che violano il regolamento.
- **Notifica di una violazione della sicurezza** (Data Breach) da parte di un Responsabile esterno.
- **Stipula di accordi o convenzioni** con altri enti (Contitolari) con i quali vengono stabilite congiuntamente le finalità e i mezzi del trattamento

3. Attività

Fase	Attività da implementare per la designazione dei Responsabili esterni	Riferimento
1. Valutazione Preliminare	Acquisire informazioni per verificare che il soggetto presenti **garanzie sufficienti** (misure tecniche e organizzative adeguate). Definire una **check-list** di verifica con il supporto del RPD.	Art. 28 GDPR
2. Procedure di Gara	Inserire nei bandi l'obbligo di possesso dei requisiti di piena conformità al GDPR come condizione per l'aggiudicazione.	Codice contratti pubblici
3. Formalizzazione	Stipulare l'**accordo ex art. 28** (scritto o elettronico) prima dell'inizio delle attività. Definire durata, natura, finalità e tipo di dati trattati.	Art. 28 GDPR
4. Censimento e Mapping	Inserire i dati del Responsabile nella Scheda Excel dedicata. Verificare la restituzione dell'accordo sottoscritto e archiviare i documenti in formato cartaceo e PDF.	Art. 28 GDPR
5. Gestione Operativa	Gestire la corrispondenza e autorizzare preventivamente l'eventuale ricorso a **sub-responsabili**. Inviare solleciti via PEC in caso di mancata conformità.	Art. 28 GDPR

6. Monitoraggio Periodico	Inviare questionari di verifica e richiedere il **Registro delle attività di trattamento** (art. 30). Controllare le scadenze contrattuali (almeno 30 giorni prima).	Art. 28 GDPR Art. 30.2 GDPR
7. Gestione Incidenti	Ricevere comunicazioni di **Data Breach** dal Responsabile e trasmetterle tempestivamente al Titolare e al referente per le violazioni.	Artt. 33-34 GDPR

Fase	Attività da implementare in caso di stipula di convenzioni/accordi di Contitolarità	Riferimento
1. Valutazione Preliminare	Acquisire informazioni per verificare che il soggetto presenti **garanzie sufficienti** (misure tecniche e organizzative adeguate). Definire una **check-list** di verifica con il supporto del RPD.	Art. 26 GDPR
2. Formalizzazione	Stipulare l'**accordo ex art. 26** (scritto o elettronico) con i Contitolari, prima dell'inizio delle attività. Definire: - Finalità del trattamento; - mezzi del trattamento (categorie di dati trattati, categorie di interessati, categorie di destinatari, durata del trattamento e periodi di conservazione dei dati, misure di sicurezza); - attribuzione dei ruoli e definizione delle rispettive responsabilità tra i diversi contitolari in merito all'osservanza del GDPR, in particolare per la gestione dei diritti degli interessati (designazione di un punto di contatto per gli interessati), le rispettive funzioni di comunicazione delle informazioni da rendere agli interessati (art13 e14 GDPR), la gestione degli incidenti di sicurezza (data breach); redazione della DPIA; procedure per la conformità e sicurezza dei trattamenti; monitoraggio e test sulle procedure adottate; procedure di comunicazione tra i diversi contitolari, ecc. - autorizzazioni al trattamento dei dati per il personale dei diversi enti coinvolti; - eventuale designazione di Responsabili esterni e sub responsabili che trattano dati per conto dei contitolari (gestori di piattaforme e applicativi, ecc.)	Art. 26 GDPR
3. Informative e Registro	Aggiornare il Registro dei trattamenti. Predisporre le informative da rendere agli interessati ex artt.13 e 14 con le informazioni relative ai Contitolari. Mettere a disposizione degli interessati il contenuto essenziale dell'accordo di contitolarità	Art. 26 GDPR
4. Censimento e Mapping	Inserire i dati dei Contitolari nella Scheda Excel dedicata. Verificare la restituzione dell'accordo di contitolarità sottoscritto e archiviare i documenti in formato cartaceo e PDF.	Art. 26 GDPR
5. Gestione Operativa	Gestire la corrispondenza e autorizzare preventivamente l'eventuale ricorso a **Responsabili** e **sub-responsabili**. Inviare solleciti via PEC in caso di mancata conformità.	Art. 28 GDPR
6. Monitoraggio Periodico	Inviare questionari di verifica e richiedere il **Registro delle attività di trattamento** (art. 30). Controllare le scadenze contrattuali (almeno 30 giorni prima).	Art. 28 GDPR Art. 30.2 GDPR
7. Gestione Incidenti	Ricevere comunicazioni di **Data Breach** dai Contitolari o dai Responsabili e trasmetterle tempestivamente al Titolare e al referente per le violazioni.	Artt. 33-34 GDPR

4. Ruoli e Responsabilità (Matrice RASCI)

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

Attività	Titolare (Sindaco)	Dirigenti/Funzionari Responsabili di Area	Persona Designata (Gestore Rapporti)	RPD (DPO)	Responsabile Esterno
Verifica garanzie e misure di sicurezza	**A/I**	**R**	**S**	**C**	**-**
Predisposizione check-list e accordi	**A/I**	**R**	**S**	**C**	**I**
Sottoscrizione Accordo Art. 28 Accordo Art. 26	**A**	**R**	**S**	**I**	**R**
Censimento e aggiornamento Excel	**A**	**I**	**R**	**I**	**-**
Invio solleciti e gestione diffide	**A**	**R**	**S**	**I**	**I**
Monitoraggio periodico (Questionari)	**A**	**R**	**S**	**C**	**R**
Segnalazione Data Breach	**A/I**	**R**	**I/S**	**C**	**R**
Parere su istruzioni illegittime	**A**	**I**	**S**	**I/C**	**R**

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.

▪ **Designato rapporti Responsabili Esterni:** Gentile Orietta Gina
▪ **Designati data breach:** Dirigente Area Amm / Saitta Antonio

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

5. Rinvio alle Istruzioni operative per il personale

Salvo quanto previsto nel presente playbook, rimane applicabile quanto già previsto nella ***Procedura per la Gestione dei Rapporti con i Responsabili esterni del trattamento*** già approvata 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.*