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: Processo di Gestione del Rischio del Trattamento

# # #

1. Titolo e Versione

- **Titolo:** *Processo di Gestione del Rischio del Trattamento*
- **Versione:** 1.0 del 04/02/2026 – approvato dall'amministrazione con delibera GC n 28 del 20/03/2026.

2. Descrizione

Il presente playbook definisce la **metodologia per l'accertamento, la valutazione e il trattamento dei rischi** relativi alla protezione dei dati personali per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Il documento stabilisce i criteri per classificare la **probabilità** e la **gravità** dell'impatto sui diritti e le libertà delle persone fisiche, integrando le misure tecniche e organizzative necessarie per garantire la conformità al GDPR e una procedura per **testare, verificare e valutare** regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

---

3. Condizioni di Attivazione

Le procedure di valutazione del rischio e della conformità devono essere eseguite nelle seguenti circostanze:

- **Pianificazione Periodica:** Almeno una volta all'anno, tipicamente entro il **30 novembre**.
- **Nuovi Trattamenti o Tecnologie:** Prima di procedere a trattamenti che prevedono l'uso di nuove tecnologie o che possono presentare un **rischio elevato**.
- **Mutamento del Contesto:** Qualora si verifichi una variazione significativa nei fattori, nella natura o nelle finalità del trattamento.
- **Richiesta del RPD:** Su istanza del Responsabile della Protezione dei Dati (DPO).
- **Logiche di Rilevamento:** Attraverso il monitoraggio continuo di **indicatori di anomalia**, quali incidenti di sicurezza (data breach), reclami degli interessati o risultanze negative di audit precedenti.

---

4. Attività

Il processo di gestione del rischio è strutturato nelle seguenti fasi operative:

1. **Definizione del Contesto [1] e Inventario:** Identificazione delle operazioni tramite il **Registro dei trattamenti**, mappatura del sistema informatico, degli applicativi e delle categorie di dati (comuni, particolari, giudiziari) e degli interessati coinvolti.
2. **Valutazione della Conformità [2] (Compliance):** Verifica del rispetto dei principi dell'Art. 5 GDPR (liceità, correttezza, trasparenza, limitazione della finalità, esattezza, minimizzazione, limitazione della conservazione, integrità, riservatezza, sicurezza) attraverso 16 quesiti specifici. In caso di "NO", significa che il principio non viene rispettato e occorre definire immediatamente misure correttive e termini di adeguamento per assicurare la conformità ai principi violati.
3. **Analisi per l'Obbligo di DPIA:** Verifica se il trattamento rientra nei casi di obbligatorietà della Valutazione d'Impatto (es. larga scala, profilazione, monitoraggio sistematico, videosorveglianza sistematica su larga scala di una zona accessibile al pubblico). Negli altri casi, se il rischio inerente è **ALTO**, la DPIA deve essere condotta comunque, prima di iniziare il trattamento.
4. **Analisi del Rischio Inerente [3]:** Valutazione dell'impatto potenziale su **Riservatezza (R), Integrità (I) e Disponibilità (D)**. Si stima la gravità dell'impatto (Basso, Medio, Alto, Molto Alto) e la probabilità che si verifichino minacce.
5. **Identificazione dei Controlli e Mitigazione:** Selezione delle misure di sicurezza appropriate (es. consultare catalogo misure ENISA) e dei responsabili per la loro attuazione entro termini prestabiliti.
6. **Valutazione del Rischio Residuo [4]:** Calcolo del rischio rimanente dopo l'applicazione delle misure pianificate. Se il rischio residuo è ancora **ALTO**, il trattamento deve essere soppresso o modificato radicalmente.[5]
7. **Monitoraggio e Audit (Compliance Test) [6]:** Esecuzione periodica di test per verificare l'efficacia delle azioni di mitigazione tramite indicatori di rischio e tecniche di campionamento.
8. **Testare, verificare e valutare l'efficacia delle misure adottate** (Audit): audit periodici a campione

[1] *l'attività può essere effettuata utilizzando il tool in Excel denominato "Tool in Excel per la Valutazione e il trattamento del rischio"*
[2] *l'attività può essere effettuata utilizzando il un tool in un file Excel denominato "tool_valutazione della conformità"*
[3] *tali valutazioni possono essere effettuate utilizzando le check list riportate nell'allegato A)*
[4] *Tale fase può essere effettuata utilizzando il Tool in Excel per la Valutazione e il trattamento del rischio*
[5] *Tale valutazione può essere fatta utilizzando le schede riportate nell'allegato B*
[6] *Tale attività può essere effettuata utilizzando la scheda riportata nell'allegato C*

---

5. Ruoli e Responsabilità (Matrice RASCI)

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

Attività / Ruolo	Titolare del Trattamento Sindaco	Funzionario/Dirigente/ Responsabile del Procedimento/Area	Personale Autorizzato	Designato d'area	RPD (DPO)
Definizione Contesto e Registro	**I**	**A**	**R**	**S**	**I/C**
Valutazione Conformità	**I**	**A**	**R**	**S**	**I/C**
Esecuzione della DPIA	**A**	**R**	**S**	**S**	**C**
Analisi del Rischio Inerente	**I**	**A**	**R**	**S**	**C**
Attuazione Misure Mitiganti	**I**	**A**	**R**	**S**	**I/C**
Monitoraggio e Compliance Test	**I**	**A**	**R (Tester)***	**R(Tester)***	**C**
Approvazione Piano di Adeguamento	**A**	**R**	**S**	**S**	**C**

Legenda:

- **R (Responsible):** Chi esegue l'attività (es. personale autorizzato o incaricati specifici).
- **A (Accountable):** Chi ha la responsabilità ultima e approva (es. Dirigente, Responsabile di Area o Titolare per atti formali).
- **S (Support):** Chi supporta l'esecuzione: Team DPIA, Designati (uno per ogni area)
- **C (Consulted):** Chi deve essere consultato obbligatoriamente (es. il RPD per pareri sulle valutazioni).
- **I (Informed):** Chi deve essere informato degli esiti (es. il Titolare o i Responsabili esterni).

**Nota: Il Tester incaricato del monitoraggio deve essere una persona diversa da quella che ha attuato le misure di mitigazione.*

6. Rinvio alle Istruzioni operative per il personale

Salvo quanto previsto nel presente playbook, rimane applicabile quanto già previsto nelle ***Processo di gestione del rischio (risk management) e metodologia di valutazione del rischio del trattamento*** approvato con delibera G.M. n. 33 del 12/05/2023**.**

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

All. A) Check list di analisi del rischio

Accesso illegittimo dei dati (violazione della Riservatezza)	
1) Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2) Quali sono le principali minacce che potrebbero concretizzare il rischio?	
3) Quali sono le fonti di rischio?	
4) Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	
5) Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6) Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fontidi rischio e alle misure pianificate?	

Modifiche indesiderate dei dati (violazione dell'Integrità)	
1) Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2) Quali sono le principali minacce che potrebbero concretizzare il rischio?	
3) Quali sono le fonti di rischio?	
4) Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	
5) Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6) Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fontidi rischio e alle misure pianificate?	

Perdita dei dati (violazione della Disponibilità)	
1) Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2) Quali sono le principali minacce che potrebbero concretizzare il rischio?	
3) Quali sono le fonti di rischio?	
4) Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	
5) Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6) Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fontidi rischio e alle misure pianificate?	

Per ognuno dei tre aspetti **valutare il livello d'impatto** in base ai criteri di seguito indicati:

Valutazione del Livello di Impatto

Indicatori del livello di impatto	
Basso	Gli individui possono andare incontro a **piccoli inconvenienti o disagi minori superabili senza particolari problemi** (tempo necessario per re-inserire informazioni, fastidi, irritazione, ecc.)
Medio	Gli individui possono andare incontro a **inconvenienti o disagi significativi**, **superabili nonostante alcune difficoltà** (costi aggiuntivi, mancato accesso a servizi aziendali, paura, difficoltà di comprensione, stress, disturbi fisici di lieve entità, ecc.)
Alto	Gli individui possono andare incontro a **conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà** (appropriazione indebita di fondi, sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, danni alla proprietà, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, citazioni in giudizio compromissione dello stato di salute, ecc.)
Molto alto	Gli individui possono andare incontro a **conseguenze significative o irreversibili**, **non superabili** (perdita capacità lavorativa, disturbi psicologici o fisici a lungo termine o cronici, decesso, ecc.)

Perdita di Riservatezza *Motivazione*		
Perdita di Integrità *Motivazione*		
Perdita di Disponibilità *Motivazione*		
Livello d'impatto più elevato		

All. B

Trattamento del rischio

Trattamento del rischio		Decisione adottata	Incaricato dell'attuazione delle misure	Termini previsti per l'attuazione/verifica
Accettazione del rischio	Il rischio viene accettato: non è necessario implementare altre misure			
Riduzione del rischio	Il rischio deve essere attenuato implementando altre misure			
Rifiuto del rischio	Il trattemento viene soppresso			
N/A	Nessun trattamento del rischio è applicabile			

Misure obbligatorie	Stato	Area/ufficio	Incaricato dell'attuazione	Termine per l'attuazione	Responsabili esterni
Obbligatoria					

All. C

COMPLIANCE TEST: FORMALIZZAZIONE

Scheda compliance test			
Rif. Test			
Data del test			
Periodo di riferimento			
Obiettivo del test			
INDICATORI DI RISCHIO UTILIZZATI			
Indicatori di esposizione al rischio	Indicatori di esposizione anomalia		Indicatori di perdita
Frequenza (periodicità)			
Popolazione	descrizione		
	#elementi		
Campione	Tecnica		
	Criterio di selezione		
Metodologia			
Tester: Cognome, nome e ruolo/ufficio di appartenenza			
ESITO			

**La compilazione della scheda, che dovrà essere datata e firmata dall'incaricato*

Validazione del rischio residuale dopo l'applicazione delle misure

L'attività di monitoraggio e verifica sopra descritta dovrà condurre ai seguenti esiti:

ESITO COMPLIANCE TEST:

POSITIVO	NEGATIVO
Non sono state rilevate anomalie o le anomalie rilevate sono giudicate non significative	Le anomalie rilevate dimostrano che le azioni poste a mitigazione non stanno mitigando il rischio
VALIDAZIONE DEL RISCHIO RESIDUO	APERTURA **PIANO DI ADEGUAMENTO**
	VALUTAZIONE RISCHIO RESIDUO

In caso di esito POSITIVO, si procederà alla VALIDAZIONE del rischio residuo (ex post) redigendo il seguente report:

VALIDAZIONE DEL RISCHIO RESIDUALE					
Descrizione	**Frequenza**	**Tester**	**Metodologia**	**Esito**	**Rischio RESIDUO (EX POST)**

In caso di esito NEGATIVO, si procederà a

- attivare un **PIANO DI ADEGUAMENTO** che descriva le criticità rilevate e indichi le azioni da mettere in atto per rimuoverle e i tempi di attuazione in base ad un cronoprogramma
- VALUTARE nuovamente il rischio inerente applicando le misure adeguate a mitigarlo seguendo la procedura descritta al punto 5).

All'esito di tali verifiche **le misure adottate**, oggetto di monitoraggio, **saranno così classificate**:

VALUTAZIONE EX POST SULLE AZIONI DI MITIGAZIONE	
NON ADEGUATA	non esiste alcuna mitigazione.
PARZIALMENTE ADEGUATA	la misura presidia solo in parte il rischio
PREVALENTEMENTE ADEGUATA	la misura presidia una parte rilevante del rischio
ADEGUATA	la misura presidia integralmente il rischio