

COMUNE DI MONTE DI PROCIDA

L'ANALISI DEI RISCHI

in attuazione del Regolamento UE 679/2016 ("GDPR")

ex artt.32



*Comune di
Monte di Procida*



SOMMARIO

L'ANALISI DEI RISCHI (ex art.32 del GDPR)	3
METODOLOGIA.....	3
Identificazione dei rischi.....	4
Identificazione delle risorse	4
Identificazione degli eventi dannosi e dei fattori di rischio	4
Classificazione dei rischi	4
Rilevazione delle misure di sicurezza esistenti	5
Analisi e valutazione dei rischi.....	5
Determinazione del livello di rischio inerente.....	5
Determinazione del livello di rischio residuo	6
Identificazione e valutazione delle opzioni per il trattamento dei rischi	7
VALUTAZIONE DEI RISCHI	7
SINTESI DELLE CRITICITÀ RILEVATE	7
CONSIDERAZIONI CONCLUSIVE ED “ACTION PLAN” (PIANO DI MIGLIORAMENTO)	7

L'ANALISI DEI RISCHI (ex art.32 del GDPR)

Di seguito è riportata la modalità di analisi dei rischi svolta, finalizzata a:

- rilevare le misure di sicurezza tecniche ed organizzative in essere, in riferimento alla sicurezza dei dati personali;
- valutarne la relativa adeguatezza;
- definire le eventuali misure da implementare per garantire il rispetto della normativa in tema di protezione dei dati personali.

Gli elementi che devono essere presi in considerazione per l'analisi e valutazione dei rischi, in conformità a quanto previsto dal Regolamento, sono principalmente:

- a) esistenza di procedure di **anonimizzazione** e **pseudonimizzazione** dei dati personali;
- b) capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;
- c) capacità di **ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) esistenza di una procedura per **testare**, **verificare** e **valutare** regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Si specifica che l'ambito dell'analisi dei rischi è da intendersi riferito esclusivamente ai dati personali e ai relativi trattamenti che gli Autorizzati/Designati svolgono su di essi nell'ambito delle attività svolte all'interno dell'Ente.

Successivamente si descrive la metodologia di riferimento da utilizzare.

METODOLOGIA

La metodologia di riferimento utilizzata è riconducibile alla Linee Guida dei principali standard internazionali per il Risk Assessment e la sicurezza dei sistemi informativi (ISO 27001:2005 e la ISO 27005), e si pone l'obiettivo di produrre risultati comparabili e riproducibili nel tempo.

Le fasi metodologiche previste dagli standard, sono le seguenti:

- identificazione dei rischi.
- analisi e valutazione dei rischi.

Si riporta di seguito il dettaglio delle relative fasi metodologiche.

Identificazione dei rischi

L'identificazione dei rischi avviene attraverso un procedimento che pone il focus sulle risorse/asset da proteggere.

Tale fase si articola nelle seguenti quattro sotto-fasi:

1. identificazione delle risorse;
2. identificazione degli eventi dannosi e dei fattori di rischio;
3. classificazione dei rischi;
4. rilevazione delle misure di sicurezza esistenti.

Di seguito il dettaglio degli obiettivi e delle attività di ciascuna sotto-fase.

Identificazione delle risorse

La sotto-fase permette di individuare tutte le risorse informative, i dati personali gestiti e i relativi trattamenti oggetto dell'analisi (Le informazioni possono essere acquisite tramite di interviste effettuate ai referenti, tramite Audit e/o a distanza).

Identificazione degli eventi dannosi e dei fattori di rischio

La sotto-fase consente di identificare, per ciascuna delle risorse precedentemente individuate, tutti gli eventi dannosi in grado di compromettere i requisiti di integrità, confidenzialità, disponibilità e affidabilità dei dati personali. Successivamente, per ciascun evento, vengono identificati i fattori di rischio, ovvero le modalità con cui gli eventi dannosi possono manifestarsi per ciascuna risorsa.

L'identificazione di eventi dannosi e fattori di rischio avviene considerando sia la specificità dell'organizzazione e dell'infrastruttura dell'Ente, sia le indicazioni fornite dall'Autorità di Controllo.

Classificazione dei rischi

La sotto-fase consente di definire le macro categorie di rischi oggetto dell'analisi, ovvero Rischi inerenti i sistemi informativi e la sicurezza dei dati, che possono essere distinti in Rischi fisici (relativi alle aree e locali dove sono disposti i sistemi e i dispositivi di comunicazione, rischi relativi all'accesso di persone nei locali medesimi, rischi relativi all'integrità e disponibilità dei sistemi ICT), Rischi logici (rischi all'integrità, riservatezza e disponibilità dei dati), Rischi di trasmissione (relativi alla sicurezza delle trasmissioni dei dati), Rischi di Compliance (relativi al mancato rispetto dei diversi adempimenti previsti dal Regolamento, ad es. nomine Responsabili e Autorizzati ai trattamenti, informative privacy, policy Data Breach, ecc.).

Rilevazione delle misure di sicurezza esistenti

La sotto-fase consente di individuare le misure di protezione esistenti per la mitigazione dei rischi. In tal senso è necessario tenere conto sia delle misure di sicurezza informatiche, sia delle misure di sicurezza fisiche ed organizzative.

Analisi e valutazione dei rischi

Nel corso di questa fase viene effettuata la misurazione del cosiddetto “**livello di rischio residuo**”, con cui si intende il rischio residuo valutato dopo aver effettuato la valutazione del sistema di controllo e delle azioni intraprese per mitigarlo. Tale fase si realizza attraverso la determinazione del livello di rischio inerente, la determinazione del livello di rischio residuo e l’identificazione e valutazione delle opzioni per il trattamento dei rischi.

Determinazione del livello di rischio inerente

Il rischio inerente è generalmente definito come il rischio connesso ad una attività e/o a un processo, a prescindere dal livello di controllo presente.

I fattori che determinano il livello di rischio inerente sono l’**impatto/gravità** (ovvero la rilevanza delle conseguenze causate dall’evento dannoso) e la **probabilità** (ovvero la possibilità che l’evento dannoso si verifichi in un periodo di riferimento). Le tabelle 1 e 2 riportano, rispettivamente, i valori di impatto e probabilità assegnati.

Tabella 1 - Assegnazione dei Valori di impatto

Impatto	Indice	Significato
Basso	10	Gli effetti dell’evento dannoso sono limitati sotto ogni punto di vista: legale, funzionale e di reputazione.
Medio	50	Gli effetti dell’evento dannoso sono circoscritti, con conseguenze significative ma sostenibili.
Alto	100	Gli effetti dell’evento dannoso possono comportare gravi conseguenze per l’organizzazione.

Tabella 2 - Assegnazione dei Valori di probabilità

Probabilità	Indice	Significato
Basso	0,1	L’evento potrebbe verificarsi al massimo una volta in un arco temporale maggiore di 10 anni.
Medio	0,5	L’evento potrebbe verificarsi più volte nell’arco temporale di 10 anni, ma non annualmente.
Alto	1	L’evento potrebbe verificarsi almeno una volta nell’arco di un anno.

L'entità del rischio inerente è data, quindi, dalla relazione tra la probabilità di accadimento dell'evento e l'impatto negativo potenziale generato. Le tabelle 3 e 4 riportano rispettivamente la valutazione e descrizione del rischio inerente.

Tabella 3 – Valutazione del rischio inerente

Livello di Rischio		Probabilità		
		Bassa	Media	Alta
Impatto	Basso	1	5	10
	Medio	5	25	50
	Alto	10	50	100

Tabella 4 - Descrizione del rischio inerente

Livello di rischio	Valore	Significato
Basso	< 10	Il livello di rischio inerente è trascurabile e non è necessario predisporre misure di controllo.
Medio	>= 10 e < 50	Il livello di rischio inerente non è trascurabile, ed è opportuno predisporre misure di controllo per la mitigazione del rischio.
Alto	>= 50	Il livello di rischio inerente è elevato, ed è necessario predisporre misure di controllo per la mitigazione del rischio.

Determinazione del livello di rischio residuo

Il rischio residuo o mitigato è generalmente definito come il rischio che rimane in seguito alla valutazione del sistema di controllo. L'entità di tale rischio si determina attraverso la combinazione di entità del rischio inerente e valutazione di adeguatezza dei controlli (o misure di protezione) in essere, come riportato nella Tabella 5.

Tabella 5 - Determinazione del rischio residuo

Rischio Residuo		Valutazione controlli		
		Adeguito	Parziale	Non Adeguato
Rischio Inerente	Basso	Basso	Basso	Medio
	Medio	Basso	Medio	Alto
	Alto	Medio	Alto	Alto

Identificazione e valutazione delle opzioni per il trattamento dei rischi

Al termine di sotto-fase, laddove si riscontri un livello di rischio residuo medio o alto, è possibile identificare ulteriori misure di sicurezza, al fine di ricondurre il rischio ad un livello di accettabilità. Tra le opzioni disponibili, è possibile accettare i rischi consapevolmente e obiettivamente, nel rispetto delle politiche aziendali. In alternativa si potrà decidere se evitare il rischio, annullando il fattore di rischio o rinunciando ad una determinata risorsa. **Da ultimo, sarà possibile decidere di trasferire il rischio ad altro soggetto, ad esempio a un'assicurazione o a un fornitore.*

REVISIONE 00

VALUTAZIONE DEI RISCHI

Matrice dei rischi

SINTESI DELLE CRITICITÀ RILEVATE

Azioni da intraprendere

Vengono riepilogati, per ciascuna tipologia di rischio residuo valutato come “MEDIO”, le azioni da intraprendere per superare le relative criticità.

CONSIDERAZIONI CONCLUSIVE ED “ACTION PLAN” (PIANO DI MIGLIORAMENTO)

Dall'analisi effettuata emerge un quadro complessivo di sostanziale adeguatezza del sistema dei controlli in essere all'interno dell'Ente, che garantisce una tutela “**Adeguate**” dei dati personali.

L'analisi, seppur sommaria, tuttavia, alcune aree di miglioramento:

-