

Valutazione del Rischio GDPR

Data di generazione: 19/12/2025 alle 17:31:16

Metodologia: Basata sulla metodologia di ENISA

1. Informazioni sulla Valutazione

Finalità del trattamento:

mkt diretto

2. Valutazione dell'Impatto

2.1 Risultati per Categoria

Categoria	Livello di Impatto	Descrizione
Riservatezza (Confidentiality)	Medio	Nessuna descrizione fornita
Integrità (Integrity)	Alto	Nessuna descrizione fornita
Disponibilità (Availability)	Molto alto	Nessuna descrizione fornita

Impatto Complessivo: Molto alto

3. Valutazione della Probabilità di Minacce

3.1 Riepilogo Risposte per Area

Area di Valutazione	Risposte Affermative	Punteggio	Livello
Risorse di rete e tecnologiche	0	1	Basso
Processi e procedure	0	1	Basso
Soggetti e persone coinvolti	0	1	Basso
Settore di attività e scala del trattamento	0	1	Basso

Punteggio Totale: 4

Probabilità delle Minacce: Basso

Descrizione: Probabilità bassa di minacce

3.2 Dettaglio Risposte

1. 1. Vi sono parti del trattamento svolte attraverso Internet?
Risposta: No

2. 2. È possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per esempio, riguardo a certi utenti o gruppi di utenti)?
Risposta: No

3. 3. Il Sistema di trattamento dati personali è interconnesso a un altro Sistema o Servizio IT interno o esterno al Vostro ente?
Risposta: No

4. 4. È facile per soggetti non autorizzati accedere all'ambiente di trattamento dati?
Risposta: No

5. 5. Il Sistema di trattamento dati personali è progettato, implementato o manutenuto senza seguire le migliori pratiche del settore?

Risposta: No

6. 6. Ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?

Risposta: No

7. 7. L'utilizzo accettabile delle risorse di rete, di Sistema e fisiche all'interno dell'ente è definito in modo incerto o insufficiente?

Risposta: No

8. 8. Ai dipendenti è consentito portare con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?

Risposta: No

9. 9. Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro dell'ente?

Risposta: No

10. 10. Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?

Risposta: No

11. 11. Il trattamento di dati personali è svolto da un numero indefinito di dipendenti?

Risposta: No

12. 12. Vi sono parti del trattamento svolte da un agente o da un soggetto terzo (responsabile del trattamento)?

Risposta: No

13. 13. Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?

Risposta: No

14. 14. Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia di sicurezza delle informazioni?

Risposta: No

15. 15. I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere i dati personali?

Risposta: No

16. 16. Ritenete che il Vostro settore di attività sia passibile di attacchi cibernetici (cyberattacks)?

Risposta: No

17. 17. L'ente ha subito attacchi cibernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?

Risposta: No

18. 18. Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?

Risposta: No

19. 19. Un trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?

Risposta: No

20. 20. Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività dell'ente che non siano state implementate in misura adeguata?

Risposta: No

4. Valutazione del Rischio Complessivo

4.1 Matrice del Rischio

	Basso impatto	Medio impatto	Alto impatto	Molto alto impatto
Alta probabilità	MEDIO	ALTO	ALTO	ALTO
Media probabilità	BASSO	MEDIO	ALTO	ALTO
Bassa probabilità	BASSO	MEDIO	ALTO	ALTO

Rischio Basso
Rischio Medio
Rischio Elevato

4.2 Rischio Finale

Rischio Complessivo: Elevato

Impatto Complessivo: Molto alto

Probabilità delle Minacce: Basso

5. Note e Considerazioni

Questa valutazione è stata effettuata utilizzando la metodologia basata sulle linee guida ENISA per la valutazione del rischio GDPR.

La matrice del rischio visualizza la correlazione tra il livello di impatto e la probabilità delle minacce.

Documento generato automaticamente dall'applicazione "Valutazione del Rischio GDPR"

Copyright Giancarlo Butti - 2025 | Compliance 4.0 - ITER

Realizzato con strumenti di AI