COMUNE DI LECCE

L'ANALISI DEI RISCHI

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

ex artt.32

Città di Lecce

SOMMARIO

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		
		Adeguato	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 01

VALUTAZIONE DEI RISCHI

Matrice dei rischi

Vedi allegato

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.

Vedi allegato

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 "***Adeguata***" dei dati personali.

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

→ revisione delle procedure di Back-up.

→ sicurezza dei dati riferiti ai documenti in Cloud;

→ raccolta e monitoraggio degli access log

→ effettuazione Penetration test

→ Formazione Autorizzati / Designati al trattamento

→ Controllo generale con Ufficio ICT

VALUTAZIONE DEI RISCHI - COMUNE DI LECCE

Matrice dei rischi

Contesto	Evento	Fattore di Rischio	Impatto / Gravità	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo	NOTE
Backup dei dati	Asportazione e furto dei back up	Inadeguatezza luogo / sistema di conservazione	M	B	B	Backup	Adeguato	Basso	Revisionare con Referente ICT
Backup dei dati	Distruzione e perdita dati	Indisponibilità dei dati	M	B	B	Backup effettuato con frequenza almeno settimanale	Adeguato	Basso	Revisionare con Referente ICT
Backup dei dati	Contenzioso con fornitore	Indisponibilità dei dati	M	B	B	Attenta scelta dei fornitori, Contratto e designazione Responsabili del trattamento	Adeguato	Basso	Revisionare con Referente ICT
Comportamento degli Autorizzati / Designati	Accessi non autorizzati ai sistemi/sedi aziendali	Inadeguatezza dei sistemi / credenziali di autenticazione	B	M	B	Autorizzazioni / Designazioni per iscritto, Disciplinare interno, Formazione e sensibilizzazione	Adeguato	Basso	Aggiornare Formazione
Comportamento degli Autorizzati / Designati	Perdita dei dati contenuti nei sistemi / depositi aziendali	Carenza di consapevolezza, incuria, disattenzione da parte dei dipendenti / collaboratori	B	B	B	Backup Adozione e controlli Codici di comportamento	Adeguato	Basso	Aggiornare Formazione
Comportamento degli Autorizzati / Designati	Furto di strumenti (e altro) contenenti dati personali	Omessa custodia	B	B	B	Codice Etico Controlli all'ingresso	Adeguato	Basso	Aggiornare Formazione
Gestione incidenti	Malfunzionamento, indisponibilità delle applicazioni	Inadeguato monitoraggio	M	M	M	Manutenzione	Parziale	Medio	Revisionare con Referente ICT
Monitoraggio dei sistemi	Malfunzionamento, indisponibilità delle applicazioni	Inadeguata rilevazione dei malfunzionamenti e degli eventi relativi ai sistemi ICT	M	B	B	Controlli informatici, Adozione Policy Data Breach	Adeguato	Basso	Revisionare con Referente ICT
Raccolta di log e monitoraggio	Manomissione log	Inadeguatezza dei sistemi di autenticazione in cui risiedono i log	B	B	B	Adozione di regole	Adeguato	Basso	Revisionare con Referente ICT
Raccolta di log e monitoraggio	Comportamenti fraudolenti da parte degli Amministratori di Sistema	Inadeguato monitoraggio sull'operato degli Amministratori di Sistema / Autorizzati che svolgono tali funzioni	A	B	M	Monitoraggio almeno semestrale degli access log degli Amministratori di sistema / Autorizzati che svolgono tali funzioni	Parziale	Medio	Revisionare con Referente ICT
Sicurezza fisica	Accessi non autorizzati agli edifici / sedi dell' azienda	Assenza di controlli e misure di protezione nelle aree che contengono informazioni sensibili o critiche	M	B	B	Presidio degli uffici / sedi, Registrazione degli ingressi (ove applicabile)	Adeguato	Basso	
Sicurezza fisica	Accessi non autorizzati agli uffici / reparti ad accesso riservato	Inadeguatezza nella gestione degli accessi (es. sala CED) Violazione sistemi antiintrusione	M	B	B	Controlli all'entrata(Badge ove applicabile), Codice Etico, Porte chiuse a chiave (ove applicabile)	Adeguato	Basso	
Sicurezza fisica	Minacce esterne ed ambientali che potrebbero provocare un indisposizione delle apparecchiature	Inadeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti	M	B	B	Antivirus, Firewall, Disaster Recovery Plan, Gruppo di continuità, manutenzione e controllo dei Server	Adeguato	Basso	Revisionare con Referente ICT
Sicurezza Data Center	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Mancanza di misure di protezione Mancanza misure di continuità	M	B	B	Manutenzione e controlli costanti	Adeguato	Basso	Revisionare con Referente ICT
Sicurezza Data Center	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	Mancanza di sistemi di alimentazione Surriscaldamento apparecchiature	M	B	B	Manutenzione periodica degli impianti Gruppo di continuità	Adeguato	Basso	Revisionare con Referente ICT
Sicurezza Data Center	Errori umani nella gestione della sicurezza fisica	Carenza di consapevolezza, incuria, disattenzione	B	B	B	Policy, Sistema disciplinare	Adeguato	Basso	Revisionare con Referente ICT
Sicurezza logica degli accessi	Accesso ai dati da parte di personale non autorizzato	Assenza di un processo per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e server Assenza di una politica di controllo degli accessi	M	B	B	Monitoraggio dei tentativi di accesso falliti, Disciplinare interno	Adeguato	Basso	Revisionare con Referente ICT
Sicurezza logica degli accessi	Perdita di riservatezza della password di accesso	Inadeguato livello di sicurezza della Password	M	B	B	Adozione di regole di Autenticazione in linea con le best practices internazionali (>8 caratteri; alfanumerica, non deve correlata a informazioni personali (ex nome ad esempio, la data di nascita, ecc.), cambio password ogni 90/180 gg, Disciplinare interno, formazione	Adeguato	Basso	Revisionare con Referente ICT, Aggiornare formazione
Sicurezza dei dati	Furto di dati	Carenza di consapevolezza, incuria, disattenzione	B	B	B	Dati protetti	Adeguato	Basso	
Sicurezza dei dati	Accesso non autorizzato ai dati da parte dei Fornitori	Assenza di una policy e mancata nomina Responsabili del trattamento	M	B	B	attenzione nella scelta dei fornitori, Designazioni Responsabili del trattamento	Adeguato	Basso	
Sicurezza della rete	Perdita dei dati di rete	Mancanza copie di sicurezza	M	B	B	Backup	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza della rete	Attacco Virus, Malware	Mancanza di controlli e software di contrasto dei codici malevoli	M	B	B	Firewall, Antivirus, Antispam	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza della rete	Errore di elaborazione	Errata gestione, modifica o aggiornamento programmi	M	B	B	Test degli aggiornamenti o modifiche evolutive	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza degli applicativi	Malfunzionamento, indisponibilità o degrado delle apparecchiature	Mancato aggiornamento	M	B	B	Aggiornamento periodico	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza degli applicativi	Accesso non autorizzato a sistema informativo	Inadeguatezza sistemi di autenticazione	M	B	B	Credenziali di accesso, Disciplinare interno	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza degli applicativi	Furto o perdita di dati	Apparecchiature incustodite / non protette	M	B	B	Sicurezza degli Uffici, Backup	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza logica	Azione di virus informatici o di programmi suscettibili di provocare danno	Mancanza di software di contrasto	A	B	M	Antivirus / Firewall Penetration test, Backup, Policy Data Breach	Parziale	Medio	Revisionare con Referente / Ufficio ICT
Sicurezza logica	Spamming o tecniche di sabotaggio	Insufficienti di policy di sicurezza	B	B	B	Antispam, Disciplinare interno	Adeguato	Basso	Aggiornare formazione
Sicurezza logica	Malfunzionamento, degrado o indisponibilità delle applicazioni	Mancato aggiornamento	B	B	B	Aggiornamento periodico dei SW	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza logica	Accessi esterni non autorizzati	Inadeguatezza dei sistemi di autenticazione	M	B	B	Adozione di regole di Autenticazione, Disciplinare iinterno	Adeguato	Basso	Aggiornare formazione
Gestione degli asset	Furto e perdita dei dati	Divulgazione di dati	M	B	B	Controllo e manutenzione (Crittografia) dei supporti magnetici	Adeguato	Basso	Revisionare con Referente / Ufficio ICT
Sicurezza workstation	Installazione di software o dispositivi atti al sabotaggio o all'intercettazione delle informazioni	Insufficienti di policy e disciplinari interni	B	B	B	Antispam, disciplinare interno, Formazione	Adeguato	Basso	Revisionare con Referente ICT, Aggiornare formazione
Sicurezza workstation	Distruzione e perdita dati	Mancanza di copie di sicurezza	B	B	B	Backup	Adeguato	Basso	Revisionare con Referente ICT

CRITICITÀ RILEVATE - COMUNE DI LECCE

Azioni da intraprendere

Contesto	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo	NOTE	Risposta al rischio residuo			
					Accettato	Ridotto	Evitato	Trasferito
Backup dei dati	Backup effettuato con frequenza almeno settimanale	Parziale	Medio	Revisionare con Referente ICT		Revisione della procedura di Bac-up in essere + Disaster recovery + controllo sistemi e applicativi Cloud		
Gestione incidenti	Manutenzione	Parziale	Medio	Revisionare con Referente ICT		Controllo Monitoraggio dei log		
Raccolta di log e monitoraggio	Monitoraggio almeno semestrale degli access log degli Amministratori di sistema / Autorizzati che svolgono tali funzioni	Parziale	Medio	Revisionare con Referente ICT			Individuazione AdS + Aggiornamento Formazione	
Sicurezza fisica	Antivirus, Firewall, Disaster Recovery Plan, Gruppo di continuità, manutenzione e controllo dei Server	Adeguato	Basso	Revisionare con Referente ICT		Controllo generale sistemi anti-intrusione		
Sicurezza Data Center	Manutenzione e controlli costanti	Adeguato	Basso	Revisionare con Referente ICT		Controllo con Ufficio ICT		
Sicurezza della rete	Test degli aggiornamenti o modifiche evolutive	Adeguato	Basso	Revisionare con Referente / Ufficio ICT		Controllo con Ufficio ICT		
Sicurezza degli applicativi	Sicurezza degli Uffici, Backup	Adeguato	Basso	Revisionare con Referente / Ufficio ICT		Controllo con Ufficio ICT		
Sicurezza logica	Antivirus / Firewall Penetration test, Backup, Policy Data Breach	Parziale	Medio	Revisionare con Referente / Ufficio ICT			Controllo generale sistemi + Svolgimento Penetration test	