Analisi dei rischi nell'ambito della gestione documentale e misure organizzative e tecniche adottate

Minaccia	Misura implementata	
Accesso non autorizzato ai documenti e ai dati in essi contenuti	Accesso al SdPG da parte di personale non autorizzato	• L'accesso al SdPG avviene, per le applicazioni di tipo web, per mezzo del trasferimento automatico delle credenziali utente acquisite al momento dell'autenticazione al dominio, mentre, per le applicazioni di tipo client / server, per mezzo di codice utente e password. • Il mancato accesso al SdPG per un periodo superiore ai sei mesi comporta la decadenza delle credenziali dell'utente interessato che deve richiederne la riattivazione. • L'accesso al SdPG è consentito solamente agli utenti esplicitamente autorizzati e la fruizione di funzioni ed informazioni è condizionata dal tipo di abilitazione attribuita ad ogni utente. • Le abilitazioni sono legate all'associazione ad una o più strutture pertanto le stesse vengono meno al momento della rimozione dell'associazione del dipendente dalle strutture stesse. • Sono impartite istruzioni specifiche al personale che utilizza l'SdPG affinché non comunichi ad altri o dia evidenza delle credenziali di accesso al proprio computer e agli applicativi in uso.
	Accesso ai documenti contenenti dati personali da parte di personale non autorizzato	• Nel SdPG sono presenti, per ogni utente, le informazioni che determinano la disponibilità delle funzioni applicative e la possibilità di accedere ai dati ed ai documenti archiviati nel sistema. • Sono impartite istruzioni specifiche al personale dell'Ente affinché la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, venga ritirata tempestivamente. • Sono impartite istruzioni specifiche al personale dell'Ente affinché non lasci incustoditi i documenti contenenti dati personali.

		• Sono impartite istruzioni specifiche al personale dell'Ente affinché al termine del turno di lavoro conservi i documenti contenenti dati personali in archivi ad accesso controllato e quelli contenenti categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR in armadi muniti di serratura.
	Accesso ai locali fisici da parte di personale non autorizzato	• L'accesso fisico alle sedi dell'Ente è controllato. • La sede principale dell'Ente è dotata di un sistema di telecamere che controlla il perimetro esterno e presenta un servizio di guardiania o di portierato. • Le stanze dove ha luogo la protocollazione, alla fine del turno di lavoro, vengono chiuse a chiave.
	Accesso alle postazioni di lavoro da parte di personale non autorizzato	• Sono impartite istruzioni specifiche al personale dell'Ente affinché non salvi documenti contenenti dati personali sulle risorse locali o li cancelli a fine turno di lavoro. • Sono impartite istruzioni specifiche al personale dell'Ente affinché non comunichi ad altri o dia evidenza delle credenziali di accesso al proprio computer e agli applicativi in uso. • Sono impartite istruzioni specifiche al personale dell'Ente affinché impedisca l'accesso al proprio computer in caso di assenza momentanea dalla propria postazione o al termine del turno di lavoro.
	Errato smistamento ad un ufficio regionale di documenti contenenti dati personali	• Sono impartite istruzioni specifiche al personale dell'Ente addetto alla protocollazione affinché minimizzi la comunicazione di dati personali qualora non sia certo della struttura destinataria della comunicazione • Sono impartite istruzioni specifiche ai responsabili delle strutture affinché, in caso di errata ricezione di documenti contenenti dati personali, procedano alla restituzione nel più breve tempo possibile e senza conservarne copia.
	Errata assegnazione ad un funzionario regionale di documenti contenenti dati personali	• Sono impartite istruzioni specifiche al personale dell'Ente affinché, in caso di errata ricezione di documenti

		contenenti dati personali, proceda alla restituzione nel più breve tempo possibile e senza conservarne copia.
Alterazione o manomissione dei documenti o dei dati in essi contenuti	• Vengono memorizzate le attività di aggiornamento dei dati di protocollo con evidenza dell'utente che le ha effettuate. • Vengono memorizzati gli accessi e le operazioni effettuate dagli Amministratori di Sistema.	
Distruzione o perdita dei documenti o dei dati in essi contenuti	• Sono presenti sistemi di backup e restore volti a garantire l'integrità e il ripristino della disponibilità dei documenti gestiti dal SdPG.	
Trattamento illecito dei dati personali	• Sono impartite istruzioni specifiche al personale dell'Ente affinché l'accesso sia limitato ai dati strettamente necessari all'esercizio delle proprie mansioni. • Sono impartite istruzioni specifiche al personale dell'Ente affinché raccolga e registri i dati personali solamente per scopi determinati, espliciti e legittimi.	
Trasmissione non autorizzata a soggetti terzi dei dati personali	• Sono impartite istruzioni specifiche al personale dell'Ente affinché comunichi, diffonda o trasferisca all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente. • Sono impartite istruzioni specifiche al personale dell'Ente affinché si astenga dal comunicare a terzi, al di fuori dell'ambito lavorativo, qualsivoglia dato personale • Sono impartite istruzioni specifiche al personale dell'Ente affinché fornisca dati e informazioni relativi a terzi solo dietro specifica autorizzazione del Titolare e non fornisca dati e informazioni ai diretti interessati, senza avere la certezza della loro identità. • Le informazioni relative a stati, fatti e qualità personali contenute nei documenti trasmessi all'interno dell'Amministrazione o a soggetti esterni sono limitate a quelle che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.	

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: CHITTARO MICHELA
CODICE FISCALE: CHTMHL81E65L483T
DATA FIRMA: 02/07/2025 13:16:09
IMPRONTA: 1FA6737BACD1949B6012100C70477E93CC82EB95C008230BB9FEE3ABD17A24A9
CC82EB95C008230BB9FEE3ABD17A24A9788036AB6E9BB9FD29E930F147B3A2C5
788036AB6E9BB9FD29E930F147B3A2C5528AEEDEBC54BE3E58DE8A5755CDD948
528AEEDEBC54BE3E58DE8A5755CDD948E51048A998371FFBD16408E0B238382A