					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P37S					Titolo del documento: **Politica di conformità legale e regolamentare**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controllo 5	
NIST SP 800-53 Rev. 5	PL-1, PL-2, PM-1, CA-1, AU-1	
GDPR UE	Articoli 5, 6, 32, 33	
NIS2 UE	Articoli 21(2)(a), 21(2)(f), 23	
DORA UE	Articoli 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Finalità

1.1 La presente politica definisce l'approccio dell'organizzazione per individuare, rispettare e dimostrare la conformità agli obblighi legali, regolamentari e contrattuali.

1.2 Stabilisce responsabilità chiare e misure operative per consentire all'organizzazione di adempiere ai propri obblighi di conformità, incluse la normativa in materia di protezione dei dati, i framework di cibersicurezza, gli accordi con i clienti e gli standard di certificazione.

1.3 Garantisce che, anche in assenza di una funzione di conformità dedicata, l'organizzazione possa mantenere operazioni conformi sotto il profilo legale, rispondere correttamente agli incidenti e conservare tutte le evidenze necessarie a dimostrare la conformità in sede di audit.

1.4 La presente politica è essenziale per conseguire la certificazione ISO/IEC 27001:2022 e soddisfare le aspettative esterne di clienti, autorità di vigilanza o partner.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i dipendenti, collaboratori esterni, liberi professionisti e fornitori terzi.

2.1.2 Tutti i servizi, le operazioni, i sistemi e le attività di gestione dei dati per i quali l'organizzazione deve rispettare requisiti legali o contrattuali.

2.1.3 Tutte le sedi e i dispositivi utilizzati per trattare informazioni aziendali, sia in ufficio sia da remoto o in cloud.

2.2 La presente politica copre:

2.2.1 La normativa in materia di protezione dei dati, come il GDPR UE.

2.2.2 La normativa in materia di cibersicurezza, come la NIS2 UE.

2.2.3 Gli obblighi specifici di settore, ove applicabili.

2.2.4 I contratti con i clienti, gli accordi di riservatezza e le clausole di audit.

2.2.5 Le certificazioni volontarie (ad es. ISO/IEC 27001) e le politiche interne che devono essere applicate ai fini della conformità.

3. Obiettivi

3.1 Stabilire responsabilità chiare: assegnare responsabilità definite per il monitoraggio, l'aggiornamento e l'applicazione degli obblighi legali, regolamentari e contrattuali.

3.2 Tutelare l'organizzazione: ridurre il rischio di violazioni di legge, sanzioni, violazioni dei dati personali e danni reputazionali.

3.3 Garantire la dimostrabilità della conformità: mantenere registrazioni verificabili che dimostrino come l'organizzazione adempie ai propri obblighi di conformità.

3.4 Supportare l'integrazione nelle policy: garantire che gli obblighi legali e regolamentari siano applicati in modo coerente in tutte le policy e i processi.

3.5 Gestire le eccezioni in modo trasparente: garantire che ogni eccezione di conformità sia