					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P37					Titolo del documento: **Politica di conformità legale e normativa**							
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**

1. Finalità

1.1 La presente politica stabilisce il quadro di riferimento vincolante per l'identificazione, la gestione e la conformità a tutti gli obblighi legali, normativi e contrattuali rilevanti per la sicurezza delle informazioni, la protezione dei dati personali e le funzioni operative dell'organizzazione.

1.2 L'obiettivo è prevenire situazioni di non conformità che possano comportare sanzioni, responsabilità legali, interruzioni operative, danni reputazionali o interventi da parte delle autorità di regolamentazione.

1.3 La presente politica supporta l'integrazione degli obblighi di conformità nella governance, nei processi di gestione del rischio, nei flussi operativi, nei cicli di vita dei progetti e nella progettazione dei sistemi.

1.4 Essa assicura che tutti gli obblighi rilevanti, nelle diverse giurisdizioni, nei vari settori e nei differenti ambiti normativi, siano chiaramente documentati, valutati, monitorati e applicati all'interno dell'organizzazione.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i dipartimenti, alle funzioni, alle unità organizzative e alle persone che agiscono per conto dell'organizzazione, inclusi:

2.1.1 Dipendenti a tempo indeterminato e determinato

2.1.2 Appaltatori, fornitori di servizi terzi, consulenti e tirocinanti

2.1.3 Fornitori, responsabili del trattamento o partner terzi che trattano dati, sistemi o adempimenti normativi dell'organizzazione

2.1.4 Qualsiasi processo aziendale, progetto o iniziativa soggetti a controllo legale o normativo

2.2 Gli ambiti di conformità disciplinati dalla presente politica includono, a titolo esemplificativo e non esaustivo:

2.2.1 Obblighi in materia di sicurezza delle informazioni e cybersicurezza (ad es. ISO/IEC 27001, NIS2, DORA)

2.2.2 Normativa in materia di protezione dei dati personali e privacy (ad es. GDPR, normative settoriali in materia di privacy)

2.2.3 Normative di settore (ad es. finanziario, sanitario, automobilistico, difesa)

2.2.4 Obblighi contrattuali derivanti da accordi di riservatezza, accordi sul livello di servizio (SLA) o accordi sul trattamento dei dati (DPA)

2.2.5 Requisiti legali relativi alla segnalazione degli incidenti, all'interazione con le autorità competenti e al trasferimento internazionale dei dati

3. Obiettivi

3.1 Assicurare che tutte le leggi, le normative, gli standard e gli obblighi contrattuali applicabili siano identificati, documentati, interpretati e applicati in tutta l'organizzazione.

3.2 Integrare i requisiti legali e normativi nel Sistema di gestione per la sicurezza delle informazioni (SGSI) dell'organizzazione, nei processi di gestione del rischio, negli accordi con i fornitori e nella progettazione di prodotti e servizi.

3.3 Fornire un meccanismo per il monitoraggio proattivo delle modifiche normative e per il conseguente aggiornamento dei controlli e della documentazione.

3.4 Definire responsabilità chiare in materia di presidio della conformità, escalation delle violazioni, gestione delle eccezioni e segnalazione verso l'esterno.

3.5 Assicurare la verificabilità e la sostenibilità della posizione legale e normativa dell'organizzazione durante ispezioni, indagini o riesami ai fini della certificazione.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Detiene la responsabilità strategica dell'allineamento legale e normativo a livello aziendale.

4.1.2 Riesamina e approva le decisioni di conformità ad alto rischio, incluse le accettazioni del rischio e le controversie legali.

4.2 Responsabile della conformità / legale interno / consulente legale

4.2.1 Mantiene il Registro di conformità, che elenca tutte le leggi, le normative, le certificazioni e le clausole contrattuali applicabili.

4.2.2 Conduce valutazioni dell'impatto legale per nuovi servizi, mercati o flussi di dati.

4.2.3 Fornisce l'interpretazione autorevole di leggi e normative.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 Riesame annuale della politica

9.1.1 La presente politica deve essere riesaminata almeno una volta per anno solare al fine di:

9.1.1.1 Assicurare il continuo allineamento con leggi aggiornate, standard di settore e quadri normativi

9.1.1.2 Convalidare l'efficacia operativa sulla base delle risultanze dell'audit e dello storico degli incidenti

9.1.1.3 Riflettere i cambiamenti organizzativi (ad es. nuove giurisdizioni, sistemi o linee di business)

9.2 Riesami attivati da eventi

9.2.1 Devono essere avviati riesami intermedi quando:

9.2.2 Entra in vigore o viene aggiornato un nuovo requisito legale o normativo

9.2.3 Un incidente di conformità o un audit evidenzia carenze della politica

9.2.4 L'organizzazione entra in un nuovo mercato o in una nuova linea di servizio disciplinati da distinti quadri di conformità

9.2.5 Le tendenze applicative o le indicazioni delle autorità di regolamentazione indicano variazioni della postura di rischio

9.3 Titolarità e approvazione

9.3.1 Il dipartimento legale e il Responsabile della conformità sono congiuntamente responsabili del coordinamento del processo di riesame.

9.3.2 Le revisioni finali della politica devono essere approvate dalla Direzione aziendale e registrate nel Registro delle modifiche delle politiche, con i relativi riferimenti al controllo delle modifiche e i piani di comunicazione associati.

9.4 Controllo delle versioni e comunicazione

9.4.1 Qualsiasi versione aggiornata della presente politica deve:

9.4.1.1 Includere una sintesi delle principali modifiche

9.4.1.2 Essere ridistribuita tramite canali ufficiali (ad es. portale delle politiche, Sistema di gestione dell'apprendimento, newsletter interne)

9.4.1.3 Richiedere la presa visione del personale interessato, in particolare di coloro che ricoprono ruoli in ambito legale, operativo, di sicurezza e di gestione dei fornitori

10. Politiche correlate e collegamenti

10.1 La presente politica opera congiuntamente con e rafforza le seguenti politiche del SGSI dell'organizzazione:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce i principi di governance di base che assicurano che tutte le politiche di sicurezza delle informazioni, inclusa la conformità, siano allineate ai requisiti strategici aziendali e normativi.

10.1.2 P2 – Politica sui ruoli e le responsabilità di governance: definisce le autorità decisionali, inclusi i ruoli legali e di conformità responsabili del presidio normativo e dell'accountability.

10.1.3 P6 – Politica di gestione del rischio: supporta la valutazione, l'attribuzione della titolarità e la mitigazione dei rischi di conformità legale e normativa in tutta l'organizzazione.

10.1.4 P8 – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: assicura che tutto il personale sia informato in merito alle responsabilità di conformità e riceva una formazione adeguata al proprio ruolo.

10.1.5 P12 – Politica di gestione degli asset: rafforza gli obblighi legali relativi alla gestione e alla protezione degli asset soggetti a vincoli normativi o contrattuali, inclusi quelli che coinvolgono dati personali e infrastrutture critiche.

10.1.6 P30 – Politica di risposta agli incidenti (P30): disciplina le notifiche legali obbligatorie (ad es. articolo 33 del GDPR) e le procedure di escalation in caso di violazione della conformità o di evento normativo.

10.1.7 P33 – Politica di monitoraggio dell'audit e della conformità: fornisce attività strutturate di assurance, inclusi test dei controlli e raccolta delle evidenze, richieste per la verifica interna ed esterna della conformità.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 4.2 – Comprensione delle esigenze e delle aspettative delle parti interessate: richiede l'identificazione e l'integrazione dei requisiti legali e normativi nel SGSI.

11.1.2 Clausola 5.1 – Leadership e impegno: attribuisce alla direzione la responsabilità per l'istituzione e il mantenimento della conformità legale in tutta l'organizzazione.

11.1.3 Clausola 5.3 – Ruoli, responsabilità e autorità organizzative: assicura chiarezza dei ruoli per il presidio legale e la conformità normativa.

11.1.4 Allegato A, Controllo 5.36 – Conformità ai requisiti legali, statutari, normativi e contrattuali: stabilisce il requisito di identificare e adempiere agli obblighi derivanti da leggi, normative e contratti.

11.2 ISO/IEC 27002

11.2.1 Controllo 5.36: fornisce linee guida di attuazione per mantenere un registro degli obblighi di conformità, validare i requisiti normativi e assicurare una conservazione strutturata delle evidenze.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politica e procedure di pianificazione della sicurezza: richiede che gli obblighi di conformità siano integrati nelle strutture di governance e nella documentazione.

11.3.2 PM-1 – Piano del programma di sicurezza delle informazioni: prevede i controlli normativi quale componente del più ampio programma di sicurezza.

11.3.3 CA-7 – Monitoraggio continuo: supporta il presidio dell'efficacia dei controlli nel soddisfare requisiti legali e di policy.

11.3.4 AU-9 – Protezione delle informazioni di audit: assicura che i log e le registrazioni di audit di conformità siano protetti e disponibili per l'ispezione.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 5 – Principi applicabili al trattamento: richiede un trattamento lecito delle informazioni, trasparenza e accountability.

11.4.2 Articolo 6 – Liceità del trattamento: impone basi giuridiche appropriate per tutte le attività sui dati.

11.4.3 Articolo 24 – Responsabilità del titolare del trattamento: stabilisce una responsabilità diretta nell'assicurare la conformità normativa.

11.4.4 Articolo 32 – Sicurezza del trattamento: richiede l'attuazione di misure tecniche e organizzative appropriate (TOM).

11.4.5 Articolo 33 – Notifica di una violazione dei dati personali: richiede che le violazioni dei dati personali siano segnalate entro 72 ore alle autorità competenti.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articoli 20–21: richiedono ai soggetti essenziali e importanti di attuare una governance documentata, strategie di conformità legale e riesame continuo dei rischi legali.

11.6 Regolamento UE DORA (2022/2554)

11.6.1 Articolo 5(2) – Quadro di gestione del rischio ICT: richiede l'integrazione della conformità legale nelle più ampie funzioni di gestione del rischio e di presidio.

11.6.2 Articolo 19 – Rischio ICT di terze parti: impone requisiti legali specifici per la gestione degli obblighi contrattuali e normativi che coinvolgono fornitori e piattaforme esterni.

11.7 COBIT 2019

11.7.1 APO12 – Gestire il rischio: include la conformità legale e normativa quale componente critica della governance del rischio aziendale.

11.7.2 MEA03 – Monitorare la conformità ai requisiti esterni: definisce il monitoraggio continuo, la gestione delle eccezioni e la capacità di dimostrare la conformità per tutte le forme di obblighi normativi.