					Insert Registered Legal Entity Name Here							
Document number: P37S					Document Title: **Legal and Regulatory Compliance Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Control 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
EU GDPR	Articles 5, 6, 32, 33	
EU NIS2	Articles 21(2)(a), 21(2)(f), 23	
EU DORA	Articles 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Purpose

1.1 This policy defines the organization's approach to identifying, meeting and demonstrating compliance with legal, regulatory and contractual obligations.

1.2 It establishes clear responsibilities and practical measures to enable the business to meet its compliance obligations, including data protection laws, cybersecurity frameworks, client agreements and certification standards.

1.3 It ensures that, even without a dedicated compliance function, the business can maintain legally compliant operations, respond appropriately to incidents and remain fully audit-ready.

1.4 This policy is essential to support ISO/IEC 27001:2022 certification and to meet external expectations from customers, regulators and business partners.

2. Scope

2.1 This policy applies to:

2.1.1 All employees, contractors and third-party service providers.

2.1.2 All services, operations, systems and data handling activities for which the organization is required to meet legal or contractual requirements.

2.1.3 All locations and devices used to process business information, whether office-based, remote or cloud-hosted.

2.2 This policy covers:

2.2.1 Data protection laws such as the EU GDPR.

2.2.2 Cybersecurity regulations such as the EU NIS2 Directive.

2.2.3 Sector-specific obligations, where applicable.

2.2.4 Client contracts, non-disclosure agreement (NDA) obligations and audit clauses.

2.2.5 Voluntary certifications, such as ISO 27001, and internal policies that must be enforced for compliance purposes.

3. Objectives

3.1 Establish accountability: assign clear responsibility for monitoring, updating and enforcing legal, regulatory and contractual obligations.

3.2 Protect the business: minimize the risk of legal violations, fines, data breach incidents and reputational damage.

3.3 Enable audit readiness: maintain verifiable records demonstrating how the organization meets its compliance obligations.

3.4 Support policy integration: ensure legal and regulatory obligations are enforced consistently across all policies and processes.

3.5 Manage exceptions transparently: ensure any compliance exceptions are documented, justified and approved to reduce liability exposure.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Has overall accountability for the organization's legal and regulatory compliance.

4.1.2 Maintains the Compliance Register and ensures that it remains current.

4.1.3 Reviews client contracts and ensures that specific obligations are tracked and enforced.

4.1.4 Approves exceptions to compliance obligations only where legally justifiable and supported by compensating controls.

4.2 External advisors (e.g., legal, IT or compliance consultants)

4.2.1 Support the GM in identifying applicable laws, certifications and obligations (e.g., GDPR, NIS2, ISO 27001).

4.2.2 Provide guidance on the interpretation of new regulations or changes to existing laws.

4.2.3 May support policy updates, audits or breach response where legal exposure is involved.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 Scheduled Annual Review

9.1.1 This policy must be reviewed every 12 months by the GM.

9.1.2 The review must confirm:

9.1.2.1 Continued relevance to the current legal and contractual context.

9.1.2.2 Appropriate reflection of client agreements and service obligations.

9.1.2.3 Alignment with the Compliance Register and related policies.

9.2 Event-Driven Updates

9.2.1 An immediate review is required if:

9.2.1.1 A new law or regulation becomes applicable (e.g., a new data protection requirement).

9.2.1.2 A client adds complex compliance terms to its agreement.

9.2.1.3 A breach or non-compliance incident occurs.

9.2.1.4 The company expands into a regulated market or sector.

9.3 Update Approval and Version Control

9.3.1 All updates must be documented, version-controlled and approved by the GM.

9.3.2 Historical versions must be retained for audit and legal purposes.

9.4 Communication of Changes

9.4.1 Staff and contractors must be informed of policy changes within 5 business days of approval.

9.4.2 Any affected vendors must also acknowledge updated terms before continuing service delivery.

10. Related Policies and Linkages

10.1 This policy is supported and enforced through the following SME policies:

10.1.1 P3S – Acceptable Use Policy: Prevents conduct that may violate legal or contractual terms (e.g., unauthorized file sharing).

10.1.2 P8S – Information Security Awareness and Training Policy: Informs personnel of compliance obligations and how to avoid violations.

10.1.3 P14S – Data Retention and Disposal Policy: Ensures lawful data handling practices across the information asset lifecycle.

10.1.4 P17S – Data Protection and Privacy Policy: Supports GDPR and customer data handling requirements.

10.1.5 P30S – Incident Response Policy: Defines how to respond to data breaches or compliance failures, including notification timelines.

10.1.6 P36S – Social Media and External Communications Policy: Ensures public communications do not breach legal or regulatory obligations.

10.2 Each linked policy enforces part of the compliance framework and must be applied in a coordinated manner.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.1 – Actions to Address Risks and Opportunities: Includes compliance risks.

11.1.2 Clause 8.1 – Operational Planning and Control: Requires the execution of processes that meet legal and contractual requirements.

11.2 ISO/IEC 27002

11.2.1 Control 5.36 – Provides guidance on maintaining records of obligations and ensuring appropriate responses to legal and regulatory requirements.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Policy and Procedures: Requires formal compliance policies.

11.3.2 PM-1 – Information Security Program Plan: Requires integration of legal compliance into security planning.

11.3.3 CA-1 – Assessment, Authorization, and Monitoring.

11.3.4 AU-1 – Audit Policy: Requires maintenance of compliance evidence.

11.4 EU GDPR

11.4.1 Article 5 – Data processing principles, including accountability.

11.4.2 Article 6 – Lawful basis for processing.

11.4.3 Article 32 – Security of processing.

11.4.4 Article 33 – Breach notification within 72 hours.

11.5 EU NIS2 Directive

11.5.1 Article 21(2)(a) and (f) – Internal policies for risk and regulatory control.

11.5.2 Article 23 – Enforcement and penalties for compliance failures.

11.6 EU DORA Regulation

11.6.1 Article 5(2) – ICT risk management oversight.

11.6.2 Article 9(1) – Internal governance of compliance.

11.6.3 Article 17 – Contractual arrangements with ICT service providers.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: Ensures compliance risks are tracked and addressed.

11.7.2 APO13 – Managed Security: Covers risk-based enforcement of regulatory and contractual compliance.

11.7.3 DSS01 – Managed Operations: Requires operational readiness to meet legal obligations.