					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 5.1, 6.1, 6.2, 8.1	
ISO/IEC 27002:2022	Control 5.36	
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	

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:
P37S</td><td colspan="9">Document Title:
Legal and Regulatory Compliance Policy</td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="9">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   1.1. This policy defines the organization's approach to identifying, complying with, and demonstrating adherence to legal, regulatory, and contractual obligations.
   1.2. It provides clear responsibilities and practical steps to help the business meet its compliance duties — including data protection laws, cybersecurity frameworks, client agreements, and certification standards.
   1.3. It ensures that even without a dedicated compliance team, the business can maintain legally sound operations, respond appropriately to incidents, and retain full audit readiness.
   1.4. This policy is essential for enabling ISO/IEC 27001:2022 certification and satisfying external expectations from customers, regulators, or partners.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All employees, contractors, freelancers, and third-party vendors
      2.1.2. All services, operations, systems, and data-handling activities where the organization must 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. The policy covers:
      2.2.1. Data protection laws such as the EU GDPR
      2.2.2. Cybersecurity regulations such as EU NIS2
      2.2.3. Sector-specific obligations (if applicable)
      2.2.4. Client contracts, confidentiality agreements, and audit clauses
      2.2.5. Voluntary certifications (e.g., ISO 27001) and internal policies that must be enforced for compliance
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 breaches, and reputational damage
   3.3. **Enable Audit Readiness**: Maintain verifiable records showing how the organization meets its compliance obligations
   3.4. **Support Policy Integration**: Ensure legal and regulatory duties are enforced consistently across all policies and processes
   3.5. **Manage Exceptions Transparently**: Ensure any compliance exceptions are documented, justified, and approved to avoid liability
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Holds overall accountability for the organization’s legal and regulatory compliance

[……]

Reference Standards and Frameworks

ISO/IEC 27001:2022

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

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

ISO/IEC 27002:2022

Control 5.36 – Guides the organization in maintaining records of obligations and ensuring appropriate responses to legal and regulatory needs

NIST SP 800-53 Rev.5

PL-1 – Policy and Procedures: Mandates formal compliance policies

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

CA-1 – Assessment, Authorization, and Monitoring

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

EU GDPR

Article 5 – Data processing principles, including accountability

Article 6 – Lawful basis for processing

Article 32 – Security of processing

Article 33 – Breach notification within 72 hours

EU NIS2 Directive

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

Article 23 – Enforcement and penalties for compliance failures

EU DORA Regulation

Article 5(2) – ICT risk management oversight

Article 9(1) – Internal governance of compliance

Article 17 – Contractual arrangements with ICT service providers

COBIT 2019

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

APO13 – Managed Security: Covers risk-based enforcement of regulatory and contract compliance

DSS01 – Managed Operations: Mandates operational readiness to meet legal obligations