					[Insert Registered Legal Entity Name Here]							
Document number: P37					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 4.2, 5.1, 5.3	
ISO/IEC 27002:2022	Controls 5.1, 5.36	
NIST SP 800-53 Rev.5	PL-1, PM-1, CA-7, AU-9	
EU GDPR	Articles 5, 6, 24, 32, 33	
EU NIS2	Articles 20–21	
EU DORA	Articles 5(2), 19	
COBIT 2019	APO12, MEA03	

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:
P37</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 establishes the mandatory framework for identifying, managing, and complying with all legal, regulatory, and contractual obligations relevant to the organization's information security, data privacy, and operational functions.
   1.2. The goal is to prevent non-compliance that could result in fines, legal liability, business disruption, reputational damage, or regulatory enforcement.
   1.3. This policy supports the integration of compliance mandates into governance, risk management, operational workflows, project lifecycles, and system design.
   1.4. It ensures that all relevant obligations—across jurisdictions, industry sectors, and regulatory scopes—are clearly documented, assessed, monitored, and enforced within the organization.
2. **Scope**
   2.1. This policy applies to all departments, functions, business units, and individuals acting on behalf of the organization, including:
      2.1.1. Permanent and temporary employees
      2.1.2. Contractors, consultants, and interns
      2.1.3. Third-party vendors, processors, or partners handling the organization's data, systems, or regulatory responsibilities
      2.1.4. Any business process, project, or initiative subject to legal or regulatory control
   2.2. Compliance domains governed by this policy include, but are not limited to:
      2.2.1. Information security and cybersecurity obligations (e.g., ISO/IEC 27001, NIS2, DORA)
      2.2.2. Data protection and privacy legislation (e.g., GDPR, sector-specific privacy laws)
      2.2.3. Sectoral regulations (e.g., financial, medical, automotive, defense)
      2.2.4. Contractual obligations arising from NDAs, service-level agreements (SLAs), or third-party processing agreements
      2.2.5. Legal requirements related to incident reporting, law enforcement interaction, and international data transfer
3. **Objectives**
   3.1. To ensure all applicable laws, regulations, standards, and contractual obligations are identified, documented, interpreted, and enforced across the organization.
   3.2. To integrate legal and regulatory requirements into the organization's ISMS, risk management processes, vendor agreements, and product/service design.
   3.3. To provide a mechanism for proactively monitoring regulatory change and updating controls and documentation accordingly.
   3.4. To define clear accountability for compliance oversight, violation escalation, exception handling, and external reporting.
   3.5. To ensure auditability and defensibility of the organization's legal and regulatory posture during inspections, investigations, or certification reviews.
4. **Roles and Responsibilities**
   4.1. **Executive Management**

4.1.1. Owns strategic accountability for legal and regulatory alignment across the enterprise.

4.1.2. Reviews and approves high-risk compliance decisions, including risk acceptances and legal disputes.

4.2. **Compliance Officer / General Counsel / Legal Advisor**

4.2.1. Maintains the **Compliance Obligations Register**, listing all applicable laws, standards, certifications, and contractual clauses.

[….]

11. Reference Standards and Frameworks

This policy aligns with internationally recognized frameworks, legal mandates, and industry standards that govern organizational compliance obligations.

ISO/IEC 27001:2022

Clause 4.2 – Understanding the Needs and Expectations of Interested Parties: Requires identification and integration of legal and regulatory requirements into the ISMS.

Clause 5.1 – Leadership and Commitment: Mandates executive accountability for establishing and maintaining legal compliance across the organization.

Clause 5.3 – Organizational Roles, Responsibilities, and Authorities: Ensures clarity of roles for legal oversight and regulatory compliance.

Annex A Control 5.36 – Compliance with Legal and Contractual Requirements: Establishes the requirement to identify and fulfill obligations arising from laws, regulations, and contracts.

ISO/IEC 27002:2022

Control 5.36 - Details implementation guidance for maintaining a compliance obligations register, validating regulatory requirements, and ensuring structured evidence retention.

NIST SP 800-53 Rev.5

PL-1 – Security Planning Policy and Procedures: Requires that compliance mandates are embedded into governance structures and documentation.

PM-1 – Information Security Program Plan: Mandates regulatory controls as a component of the broader security program.

CA-7 – Continuous Monitoring: Supports oversight of control effectiveness in meeting legal and policy requirements.

AU-9 – Protection of Audit Information: Ensures compliance audit logs and records are protected and available for inspection.

EU GDPR (2016/679)

Article 5 – Principles Relating to Processing: Requires lawful processing, transparency, and accountability.

Article 6 – Lawfulness of Processing: Mandates appropriate legal bases for all data activities.

Article 24 – Responsibility of the Controller: Establishes direct accountability for ensuring regulatory compliance.

Article 32 – Security of Processing: Demands implementation of appropriate technical and organizational controls.

Article 33 – Breach Notification: Requires that personal data breaches be reported within 72 hours to relevant authorities.

EU NIS2 Directive (2022/2555)

Articles 20–21: Require essential and important entities to implement documented governance, legal compliance strategies, and continuous review of legal risks.

EU DORA (2022/2554)

Article 5(2) – ICT Risk Management Framework: Requires integration of legal compliance within broader risk management and oversight functions.

Article 19 – ICT Third-Party Risk: Imposes specific legal requirements for managing contractual and regulatory obligations involving external vendors and platforms.

COBIT 2019

APO12 – Manage Risk: Incorporates legal and regulatory compliance as critical components of enterprise risk governance.

MEA03 – Monitor Compliance with External Requirements: Defines ongoing monitoring, exception handling, and audit readiness for all forms of regulatory obligations.