					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**

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 purpose is to prevent non-compliance that could result in fines, legal liability, business disruption, reputational damage, or regulatory enforcement action.

1.3 This policy supports the integration of compliance requirements into governance, risk management, operational processes, project lifecycles, and system design.

1.4 It ensures that all relevant obligations across jurisdictions, industry sectors, and regulatory domains 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 workers

2.1.2 Contractors, third-party service providers, 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 requirements

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 Sector-specific regulations (e.g., financial, medical, automotive, defense)

2.2.4 Contractual obligations arising from non-disclosure agreements (NDAs), service level agreements (SLAs), or third-party processing agreements

2.2.5 Legal requirements related to incident reporting and management, interaction with law enforcement, and international data transfers

3. Objectives

3.1 To ensure that 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 Information Security Management System (ISMS), risk management processes, vendor agreements, and product and 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 management, exception handling, and external reporting.

3.5 To ensure the organization's legal and regulatory posture is auditable and defensible during inspections, investigations, or certification audits.

4. Roles and Responsibilities

4.1 Top Management

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

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

4.2 Compliance Officer / General Manager / Legal and Compliance Officer

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

4.2.2 Conducts legal impact assessments for new services, markets, or data flows.

4.2.3 Provides authoritative interpretation of laws and standards.

[... 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 Annual Policy Review

9.1.1 This policy must be reviewed at least once per calendar year to:

9.1.1.1 Ensure continued alignment with updated laws, industry standards, and regulatory frameworks

9.1.1.2 Validate operational effectiveness based on audit findings and incident history

9.1.1.3 Reflect organizational changes (e.g., new jurisdictions, systems, or business lines)

9.2 Trigger-Based Reviews

9.2.1 Interim reviews must be initiated when:

9.2.2 A new legal or regulatory requirement is enacted or updated

9.2.3 A compliance incident or audit identifies shortcomings in the policy

9.2.4 The organization enters a new market or service line governed by distinct compliance frameworks

9.2.5 Enforcement trends or regulator guidance indicate changes in risk posture

9.3 Ownership and Approval

9.3.1 The Legal Department and Compliance Officer are jointly accountable for coordinating the review process.

9.3.2 Final policy revisions must be approved by Top Management and recorded in the Policy Change Register, with associated change control references and communication plans.

9.4 Version Control and Communication

9.4.1 Any updated version of this policy must:

9.4.1.1 Include a summary of key changes

9.4.1.2 Be redistributed through official channels (e.g., policy portal, LMS, internal newsletters)

9.4.1.3 Require acknowledgment from affected personnel, particularly those in legal, operational, security, and vendor management roles

10. Related Policies and Linkages

10.1 This policy operates in conjunction with and reinforces the following policies within the organization's Information Security Management System (ISMS):

10.1.1 P1 – Information Security Policy: Establishes the governance principles and control baseline to ensure that all information security policies, including compliance-related policies, align with strategic business and regulatory requirements.

10.1.2 P2 – Governance Roles and Responsibilities Policy: Defines decision-making authorities, including legal and compliance roles responsible for regulatory oversight and accountability.

10.1.3 P6 – Risk Management Policy: Supports the assessment, ownership, and treatment of legal and regulatory compliance risks across the enterprise.

10.1.4 P8 – Information Security Awareness and Training Policy: Ensures that all personnel are informed of their compliance responsibilities and receive role-appropriate training.

10.1.5 P12 – Asset Management Policy: Reinforces legal obligations for managing and protecting regulated or contractual assets, including those involving personal data and critical infrastructure.

10.1.6 P30 – Incident Response Policy: Governs mandatory legal notifications (e.g., GDPR Article 33) and escalation procedures in the event of a compliance breach or regulatory incident.

10.1.7 P33 – Audit and Compliance Monitoring Policy: Provides structured assurance activities, including control testing, remediation, and evidence collection, required for internal and external compliance verification.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 4.2 – Understanding the Needs and Expectations of Interested Parties: Requires the identification and integration of legal and regulatory requirements into the Information Security Management System (ISMS).

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

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

11.1.4 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.

11.2 ISO/IEC 27002

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

11.3 NIST SP 800-53 Rev. 5

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

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

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

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

11.4 EU GDPR (2016/679)

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

11.4.2 Article 6 – Lawfulness of Processing: Requires an appropriate lawful basis for all data processing activities.

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

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

11.4.5 Article 33 – Breach Notification: Requires personal data breaches to be reported to the relevant supervisory authority within 72 hours.

11.5 EU NIS2 Directive (2022/2555)

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

11.6 EU DORA (2022/2554)

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

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

11.7 COBIT 2019

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

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