					[Insert Registered Legal Entity Name Here]						
Document number: P17					Document Title: **Data Protection and Privacy 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, 6.1.3, 8.1, 10.1	
ISO/IEC 27002:2022	Controls 5.34, 8.10, 8.11, 8.12	
NIST SP 800-53 Rev.5	R-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	
EU GDPR	Articles 5, 6, 12–23, 25, 28, 30, 32–34; Recital 78	
EU NIS2	Article 21(2)(e), (f)	
EU DORA	Articles 6(2)(d), 11(1)(c), 15(1), 17	
COBIT 2019	APO12, DSS01, DSS05, MEA03	

<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P17</td><td colspan="7">Document Title:
<b>Data Protection and Privacy Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="7">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 mandatory organizational principles and technical requirements for the protection of personal data and the enforcement of privacy-by-design across all environments.

1.2 It formalizes the enterprise’s responsibilities under international standards and regulatory frameworks, ensuring that personal data is collected, processed, retained, shared, and disposed of lawfully, securely, and transparently.

1.3 This policy also reinforces compliance with applicable privacy laws and frameworks, including the EU General Data Protection Regulation (GDPR), EU NIS2 Directive, EU Digital Operational Resilience Act (DORA), ISO/IEC 27001:2022, and COBIT 2019.

2. Scope

2.1 This policy applies to all organizational units, personnel, and systems involved in the processing of personal data, including:

2.1.1 Employees, contractors, consultants, and third-party service providers.

2.1.2 Data collected from internal and external sources across all business functions.

2.1.3 Physical and digital media, including cloud services, SaaS platforms, mobile devices, and paper-based records.

2.1.4 All environments, including production, development, test, and backup systems where personal data may exist.

2.2 It covers all processing activities regulated under applicable privacy laws and standards, including but not limited to:

2.2.1 Collection, storage, use, transmission, and disposal of personal data.

2.2.2 Data subject rights enforcement, lawful basis documentation, consent management.

2.2.3 Cross-border transfers, breach notification, and third-party data sharing.

2.2.4 Secure design and default privacy enforcement in systems and processes.

3. Objectives

3.1 Ensure lawful, transparent, and accountable processing of personal data in alignment with ISO/IEC 27001:2022 and associated legal mandates.

3.2 Embed privacy-by-design and privacy-by-default principles in all information systems, services, and business processes.

3.3 Enforce technical and organizational measures (TOMs) that safeguard the confidentiality, integrity, and availability of personal data throughout its lifecycle.

3.4 Define governance roles and accountability structures for data protection, including the responsibilities of the Data Protection Officer (DPO), Information Security, Legal, and Data Owners.

3.5 Enable full compliance with GDPR Articles 5, 6, 25, 30, and 32, as well as with risk reduction and resilience requirements under NIS2 and DORA.

3.6 Uphold data subject rights, including access, rectification, erasure, restriction, portability, objection, and protection from automated decision-making.

3.7 Mitigate regulatory, reputational, legal, and operational risks arising from unauthorized access, misuse, or loss of personal data.

4. Roles and Responsibilities

4.1 Executive Management

4.1.1 Provides strategic oversight and allocates sufficient resources to support the privacy program.

4.1.2 Approves this policy and ensures its enforcement across the organization.

4.2 Data Protection Officer (DPO)

4.2.1 Acts independently to oversee compliance with data protection regulations.

[……]

11. Reference Standards and Frameworks

This policy aligns with internationally recognized standards and regulatory frameworks to ensure lawful, secure, and accountable personal data processing.

ISO/IEC 27001:2022

Clause 5.1 – Leadership and Commitment: Establishes executive-level responsibility for protecting personal data and enforcing privacy principles.

Clause 6.1.3 – Information Security Risk Treatment: Supports privacy risk identification, assessment, and treatment via DPIAs and exceptions.

Clause 8.1 – Operational Planning and Control: Requires technical and procedural safeguards to ensure personal data is processed securely.

Clause 10.1 – Continual Improvement: Mandates periodic evaluation and adaptation of the privacy program.

ISO/IEC 27002:2022 – Controls 5.34, 8.10, 8.11, 8.12. Provides guidance on handling of PII, enforcement of retention, deletion, anonymization, and transparency for subject rights.

NIST SP 800-53 Rev.5

AR-1, AR-2, AR-4, AR-5 – Define governance, roles, accountability, and privacy training responsibilities.
PL-2, PL-8 – Require integration of privacy controls into system lifecycle and enterprise architecture.
AC-2, AC-6 – Enforce least privilege and account management for personal data protection.
AU-2, AU-6, AU-9 – Mandate logging, traceability, and audit integrity for personal data access.
IR-4, IR-5, IR-6 – Define structured detection, analysis, and reporting processes for privacy breaches.
PM-1, PM-21, PM-23 – Establish a comprehensive privacy program, aligned with strategic risk and data governance objectives.

EU GDPR (2016/679)

Articles 5, 6, 12–23, 25, 28, 30, 32–34: Governs lawful processing, purpose limitation, data subject rights, accountability, data protection by design and by default, third-party obligations, and breach management.

Recital 78: Reinforces privacy-by-design principles.

EU NIS2 Directive (2022/2555)

Article 21(2)(e) and (f): Requires implementation of risk-based security controls and protection of personal data under essential and important entities' scope.

EU DORA (2022/2554)

Article 6(2)(d) – Enforces internal governance for ICT risk relating to data handling.

Article 11(1)(c) – Mandates third-party risk oversight for data-related services.

Articles 15(1) and 17 – Require secure data processing by service providers and timely supervisory disclosures following ICT-related incidents.

COBIT 2019

APO12 – Risk Management: Embeds privacy risk into broader enterprise risk oversight.

DSS01 – Managed Operations and **DSS05 – Security Services**: Ensure secure operations including access control, retention, and system integrity.

MEA03 – Compliance Monitoring: Requires ongoing review of compliance status against regulatory and policy-based privacy obligations.