<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P17S</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>

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	
ISO/IEC 27002:2022	Controls 5.34, 8.10–8.12	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
EU GDPR	Article 5, 6, 12-23, 30, 32-34	
EU NIS2	Article 21(2)(e), 21(2)(f)	
EU DORA	Articles 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

					[Insert Registered Legal Entity Name Here]						
Document number: P17S					Document Title: **Data Protection and Privacy Policy**						
Version: 1.0		Effective Date: 01.01.2025			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

1. **Purpose**
   1.1. This policy defines how the organization protects personal data in line with legal obligations, regulatory frameworks, and international security standards.
   1.2. It ensures that personal data—whether from customers, staff, or partners—is collected, used, stored, and deleted in a lawful, fair, and secure way.
   1.3. This policy also enables compliance with ISO/IEC 27001:2022 and supports audit readiness by enforcing a consistent, risk-based approach to privacy protection.
   1.4. Through this policy, the organization demonstrates accountability and builds customer trust by prioritizing transparency, data minimization, and strong privacy governance.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All employees, contractors, or service providers who access, process, or manage personal data
      2.1.2. Any system, application, or location where personal data is stored or transmitted
      2.1.3. All personal data, whether stored electronically, on paper, in cloud systems, or mobile devices
   2.2. This policy applies to data related to customers, staff, vendors, and any other identifiable individuals.
   2.3. The policy remains in force regardless of whether data is processed internally or by third-party service providers.
3. **Objectives**
   3.1. Ensure personal data is handled in accordance with privacy laws and security standards, including GDPR, NIS2, and ISO 27001.
   3.2. Protect personal data against unauthorized access, misuse, alteration, or loss through clear technical and organizational controls.
   3.3. Respect the privacy rights of individuals, including the right to access, correct, and erase their data.
   3.4. Establish clear roles and responsibilities for data protection within the organization.
   3.5. Enforce data minimization, secure retention, and timely deletion across all systems and processes.
   3.6. Reduce the risk of non-compliance, legal penalties, reputational damage, or customer distrust.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Approves this policy and ensures it is enforced
      4.1.2. Provides necessary resources to manage privacy risks and respond to incidents
      4.1.3. Holds overall accountability for compliance with privacy laws and standards
   4.2. **Privacy Coordinator (Internal or Outsourced)**
      4.2.1. Maintains data processing activity records
      4.2.2. Responds to individual privacy requests and regulatory inquiries
      4.2.3. Supports risk assessments, training, and policy implementation
      4.2.4. Documents breach cases and notifies authorities when required
   4.3. **IT Support Provider**
      4.3.1. Applies encryption, access controls, secure storage, and backups
      4.3.2. Limits system access to authorized users only

4.3.3. Configures privacy-by-default settings in systems and applications

4.4. **Department Managers**

4.4.1. Ensure staff follow privacy rules when collecting or handling personal data

4.4.2. Verify that data is stored securely and only for authorized purposes

[……….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 5.1 – Requires top management to demonstrate leadership and commitment to protecting personal data.

Clause 6.1.3 – Mandates treatment of risks related to processing personal information.

Clause 8.1 – Requires implementation of operational controls to safeguard data throughout its lifecycle.

ISO/IEC 27002:2022

Control 5.34 – Provides implementation guidance on protecting privacy and handling PII securely.

Control 8.10 – Addresses secure disposal of personal data to prevent residual disclosure.

Control 8.11 – Supports use of masking and pseudonymization for data minimization.

Control 8.12 – Prevents unauthorized data leakage through controls on data access and use.

NIST SP 800-53 Rev.5

AR-2 – Assigns roles and responsibilities for managing privacy risk.

PL-5 – Requires privacy plan documentation covering data use and protection.

AC-6 – Mandates least privilege and access controls for personal data.

IR-4 – Requires incident handling processes for breaches involving personal data.

EU GDPR

Article 5 – Defines the core principles of lawful, fair, and transparent data processing.

Article 6 – Requires valid legal basis for each personal data processing activity.

Articles 12–23 – Outline data subject rights including access, rectification, erasure, and objection.

Article 30 – Mandates records of processing activities.

Article 32 – Requires appropriate technical and organizational security measures.

Articles 33–34 – Set breach notification obligations to authorities and data subjects.

EU NIS2

Article 21(2)(e) – Requires measures to ensure data protection aligned with cybersecurity policies.

Article 21(2)(f) – Mandates mechanisms to manage the security of personal and confidential data in ICT systems.

EU DORA

Article 6 – Requires internal governance frameworks that manage data risk and protection.

Article 15 – Obligates financial entities to ensure third-party providers protect personal data and support regulatory compliance.

Article 17 – Requires firms to ensure that ICT systems processing personal data are secure, resilient, and monitored.

COBIT 2019

APO12 – Manage Risk: Requires identification and treatment of privacy and data protection risks.

DSS05 – Manage Security Services: Mandates safeguards to prevent unauthorized access to personal data.

MEA03 – Monitor Compliance: Requires organizations to ensure ongoing compliance with privacy and data protection laws.