					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	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Controls 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
EU GDPR	Articles 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, MEA	

1. Purpose

1.1. This policy defines how the organization protects personal data in accordance with legal obligations, regulatory frameworks, and international security standards.

1.2. It ensures that personal data—whether relating to customers, personnel, or partners—is collected, used, stored, and deleted lawfully, fairly, and securely.

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 protection and data minimization, and strong privacy governance.

2. Scope

2.1. This policy applies to:

2.1.1. All employees, contractors, and service providers who access, process, or manage personal data

2.1.2. Any system, application, or location in which personal data is stored or transmitted

2.1.3. All personal data, whether stored electronically, in paper form, in cloud systems, or on mobile devices

2.2. This policy applies to data relating to customers, personnel, vendors, and any other identifiable individuals.

2.3. This policy remains in force regardless of whether data is processed internally or by contractors and 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 clearly defined technical and organizational controls.

3.3. Respect the privacy rights of individuals, including the rights to access, rectify, and erase their data.

3.4. Establish clear roles and responsibilities for data protection within the organization.

3.5. Enforce data protection and data minimization, secure retention, and timely deletion across all systems and processes.

3.6. Reduce the risk of non-compliance, legal penalties, reputational damage, and loss of customer trust.

4. Roles and Responsibilities

4.1. General Manager (GM)

4.1.1. Approves this policy and ensures its enforcement

4.1.2. Provides the resources necessary to manage privacy risks and respond to incidents

4.1.3. Retains overall accountability for compliance with privacy laws and standards

4.2. Privacy Coordinator (Internal or Outsourced)

4.2.1. Maintains records of processing activities

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 personal data breach cases and notifies authorities where required

[... 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. Scheduled Reviews

9.1.1. This policy must be reviewed at least once every 12 months by the Privacy Coordinator and approved by the General Manager

9.1.2. The review must assess the policy's continued relevance, regulatory alignment, and operational effectiveness

9.2. Triggers for Interim Review

9.2.1. Policy updates must also be initiated in response to:

9.2.1.1. New or revised data protection laws (e.g., GDPR, DORA)

9.2.1.2. Security incidents or privacy breaches involving personal data

9.2.1.3. Implementation of new systems, tools, or services that process personal data

9.2.1.4. Material audit findings or regulator recommendations

9.3. Change Control and Communication

9.3.1. All changes to this policy must be formally documented in a change log

9.3.2. Revised versions must be distributed to all employees and applicable contractors

9.3.3. Archived versions must be retained to support compliance audit trails

10. Related Policies and Linkages

10.1. This policy operates in conjunction with other SME policies to create a complete and enforceable privacy framework:

10.1.1. P13S – Data Classification and Labeling Policy: Ensures that personal data is appropriately classified so that privacy protections can be applied based on risk.

10.1.2. P14S – Data Retention and Disposal Policy: Provides clear requirements for how long personal data must be retained and the secure methods for its disposal once no longer required.

10.1.3. P16S – Data Masking and Pseudonymization Policy: Specifies how personal identifiers must be transformed before data is used in non-production environments or shared externally.

10.1.4. P30S – Incident Response Policy: Defines the steps required to respond to personal data breaches, including notification of regulators and affected individuals within required timeframes.

10.1.5. P2S – Governance Roles & Responsibilities Policy: Clarifies the accountability structure and decision-making roles that apply to privacy enforcement and oversight.

10.2. These related policies must be reviewed and applied together to ensure end-to-end privacy coverage across systems, personnel, and suppliers.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

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

11.1.2. Clause 6.1.3 – Requires the treatment of risks related to the processing of personal information.

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

11.2. ISO/IEC 27002

11.2.1. Control 5.34 – Provides implementation guidance on protecting privacy and handling personally identifiable information (PII) securely.

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

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

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

11.3. NIST SP 800-53 Rev.5

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

11.3.2. PL-5 – Requires documented privacy plans covering data use and protection.

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

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

11.4. EU GDPR

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

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

11.4.3. Articles 12–23 – Set out data subject rights, including access, rectification, erasure, and objection.

11.4.4. Article 30 – Requires records of processing activities.

11.4.5. Article 32 – Requires appropriate technical and organizational controls.

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

11.5. EU NIS2

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

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

11.6. EU DORA

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

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

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

11.7. COBIT 2019

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

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

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