					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 5.1, 6.1.3, 8.1, 10	Relevant general, technical, continual improvement, and data protection controls
ISO/IEC 27002:2022	Controls 5.34, 8.10, 8.11, 8.12	Controls for handling PII, retention, deletion, anonymization, and data subject rights
NIST SP 800-53 Rev.5	AR-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	Governance, risk, access management, logging, breach response, and privacy program requirements
EU GDPR	Articles 5, 6, 12–23, 25, 28, 30, 32–34; Recital 78	Core privacy, accountability, data subject rights, DSRs, breach management, and design and default principles
EU NIS2	Article 21(2)(e), (f)	Risk-based security controls for essential and important entities
EU DORA	Articles 6(2)(d), 11(1)(c), 15(1), 17	Governance, third-party risk, and secure processing requirements
COBIT 2019	APO12, DSS01, DSS05, MEA	Risk management, secure operations, and compliance oversight

1. Purpose

1.1 This policy establishes mandatory organizational control principles and technical requirements for the protection of personal information (PII) and the implementation of privacy by design across all environments.

1.2 It formalizes the enterprise's responsibilities under international standards and regulatory frameworks, ensuring that personal information (PII) 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 information (PII), including:

2.1.1 Employees, contractors, 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 information (PII) 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 information (PII).

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

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

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

3. Objectives

3.1 Ensure lawful, transparent, and accountable processing of personal information (PII) in alignment with ISO/IEC 27001:2022 and applicable legal requirements.

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

3.3 Implement technical and organizational measures (TOMs) that protect the Confidentiality, Integrity, and Availability of personal information (PII) 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 Compliance, and Data Owners.

3.5 Enable full compliance with GDPR Articles 5, 6, 25, 30, and 32, as well as risk reduction and ICT 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 risk arising from unauthorized access to, misuse of, or loss of personal information (PII).

4. Roles and Responsibilities

4.1 Top 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.

4.2.2 Maintains the Record of Processing Activities (RoPA) in accordance with GDPR Article 30.

4.2.3 Leads regulatory engagement, conducts Data Protection Impact Assessments (DPIAs), and manages breach notification processes.

4.2.4 Reviews privacy exceptions and maintains the Privacy Exception Register.

[... 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 This policy shall be reviewed at least annually or earlier under the following conditions:

9.1.1 Significant legal or regulatory updates (e.g., amendments to GDPR, DORA deadlines)

9.1.2 New systems or processing activities involving personal information (PII)

9.1.3 Internal audit findings indicating policy gaps

9.1.4 Material breach incidents or supervisory authority feedback

9.2 Review Responsibilities

9.2.1 The Data Protection Officer (DPO) shall initiate the policy review, coordinating with Legal and Compliance, Risk, Information Security, and Top Management.

9.2.2 All updates shall be recorded in the ISMS Document Control Register and distributed to affected stakeholders.

9.3 Change Control

9.3.1 Any revision to this policy shall be formally approved by Top Management.

9.3.2 Obsolete versions shall be archived securely, and the updated version shall include a documented Change Log.

10. Related Policies and Linkages

10.1 P1 – Information Security Policy. Establishes the overarching security governance principles that underpin this privacy policy. P1 supports the Confidentiality, Integrity, and Availability of personal information (PII) across all systems and services.

10.2 P6 – Risk Management Policy. Defines the organization's risk treatment methodology, which is essential for assessing privacy risks, Data Protection Impact Assessment (DPIA) processes, and residual risk evaluations required under GDPR and ISO/IEC 27001 Clause 6.1.3.

10.3 P13 – Data Classification and Labeling Policy. Guides the classification of personal and sensitive data, forming the basis for applying appropriate privacy controls, including retention enforcement, access limitation, and secure disposal.

10.4 P14 – Data Retention Policy and Secure Disposal Policy. Directly supports privacy requirements under GDPR Articles 5(1)(e) and 17, ensuring that personal information (PII) is retained only as long as necessary and disposed of securely in line with legal obligations.

10.5 P16 – Data Masking and Pseudonymization Policy. Establishes controls for reducing the identifiability of personal information (PII) through technical measures such as tokenization, dynamic masking, and pseudonymization, thereby supporting Article 32 of the GDPR and Control 5.34 of ISO/IEC 27002.

10.6 P30 – Incident Response Policy. Outlines the mandatory breach response protocols that integrate with the privacy breach handling and notification timelines required under GDPR Articles 33 and 34.

10.7 P33 – Audit and Compliance Monitoring Policy. Establishes scheduled assessments of privacy program effectiveness, policy enforcement, and corrective action tracking across organizational units and third-party processors.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 5.1 – Leadership and Commitment: Establishes executive-level responsibility for protecting personal information (PII) and enforcing privacy principles.

11.1.2 Clause 6.1.3 – Information Security Risk Treatment: Supports privacy risk identification, assessment, and treatment through Data Protection Impact Assessments (DPIAs) and exceptions.

11.1.3 Clause 8.1 – Operational Planning and Control: Requires technical and procedural safeguards to ensure personal information (PII) is processed securely.

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

11.2 ISO/IEC 27002:2022 Controls 5.34, 8.10, 8.11, 8.12: Provides guidance on handling personal information (PII), retention, deletion, anonymization, and transparency for data subject rights.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Define governance, roles, accountability, and privacy training responsibilities.

11.3.2 PL-2, PL-8: Require integration of privacy controls into the system lifecycle and enterprise architecture.

11.3.3 AC-2, AC-6: Enforce least privilege and account management for protection of personal information (PII).

11.3.4 AU-2, AU-6, AU-9: Require logging, traceability, and audit integrity for access to personal information (PII).

11.3.5 IR-4, IR-5, IR-6: Define structured detection, analysis, and reporting processes for privacy breaches.

11.3.6 PM-1, PM-21, PM-23: Establish a comprehensive privacy program aligned with strategic risk and data governance objectives.

11.4 EU GDPR (2016/679)

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

11.4.2 Recital 78: Reinforces privacy by design principles.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(e) and (f): Requires implementation of risk-based security controls and protection of personal information (PII) within the scope of essential and important entities.

11.6 EU DORA (2022/2554)

11.6.1 Article 6(2)(d): Requires internal governance for ICT risk relating to data handling.

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

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

11.7 COBIT 2019

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

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

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