					[Insert Registered Legal Entity Name Here]							
Document number: P14S					Document Title: **Data Retention and Disposal 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 6.1.3, 8.1	
ISO/IEC 27002:2022	Control 5.33	
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	
EU NIS2	Article 21(2)(a)	
EU DORA	Article 5(1)	
COBIT 2019	BAI03.04, DSS01.06	
EU GDPR	Article 5(1)(e), 17	

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:
P14S</td><td colspan="9">Document Title:
Data Retention and Disposal Policy</td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="9">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. The purpose of this policy is to define enforceable rules for the retention and secure disposal of information within an SME environment. It ensures records are kept only for the duration required by law, contractual obligation, or business necessity—and securely destroyed thereafter.
   1.2. This policy aims to reduce information risk, manage legal exposure, and limit storage of redundant or obsolete data. It helps ensure compliance with ISO/IEC 27001 and privacy frameworks such as GDPR by minimizing unauthorized retention of personal or sensitive information.
   1.3. A well-structured retention and disposal framework reduces operating costs, improves system performance, and increases audit readiness. For SMEs with constrained IT capacity, it provides a practical way to manage digital and physical information assets responsibly.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All records, files, logs, communications, and data sets created, collected, processed, or stored by the organization
      2.1.2. All employees, contractors, and external providers handling organizational data
      2.1.3. All data formats (e.g., paper, electronic, image, audio, or log) and all storage media (e.g., local drives, cloud services, email servers, backups)
   2.2. The scope includes:
      2.2.1. Business documents (e.g., invoices, contracts, project reports)
      2.2.2. Operational records (e.g., logs, access history, backup snapshots)
      2.2.3. Personal data (e.g., HR files, client communications, support records)
      2.2.4. Data hosted internally, externally, or in hybrid systems
      2.2.5. Archived and backup data, whether active or dormant
   2.3. All stages of the data lifecycle are in scope—from creation to authorized disposal.
3. **Objectives**
   3.1. Define consistent retention rules based on legal, operational, and regulatory criteria.
   3.2. Prevent premature deletion of critical records and eliminate unnecessary data accumulation.
   3.3. Ensure secure, irreversible disposal of data when retention is no longer required.
   3.4. Assign ownership for enforcing retention and deletion decisions within SME-level staffing constraints.
   3.5. Provide audit-ready documentation to demonstrate due diligence under ISO 27001, GDPR, NIS2, and other frameworks.
   3.6. Promote secure lifecycle handling of data without imposing unnecessary technical burden on non-specialist personnel.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Approves and owns this policy.
      4.1.2. Ensures retention and disposal procedures are implemented in a manner consistent with legal and business risk.
      4.1.3. Authorizes exceptions and legal holds when necessary.

4.1.4. Initiates policy reviews and approves updates based on business or regulatory changes.

4.2. **Designated Data Owner**

4.2.1. Assigned per data category (e.g., financial, HR, client records).

4.2.2. Classifies records and determines appropriate retention based on policy and legal guidance.

4.2.3. Authorizes deletion when retention requirements are fulfilled.

4.2.4. Supports internal audits by providing context on retention logic and disposal events.

4.3. **IT Support Provider / Internal IT Lead**

4.3.1. Configures systems to support automated retention enforcement and secure deletion.

4.3.2. Implements tools for data sanitization and destruction.

4.3.3. Maintains logs of disposal events.

4.3.4. Ensures backup systems and archived media are subject to the same retention limits.

4.4. **All Employees and Contractors**

4.4.1. Must comply with this policy's retention rules.

4.4.2. Must not retain records longer than permitted or delete them prematurely.

4.5. […….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 6.1.3: Requires treatment of information-related risks, including retention risks.

Clause 8.1: Defines lifecycle operational controls.

ISO/IEC 27002:2022

Control 5.33: Provides guidance for setting retention periods and choosing secure destruction methods.

NIST SP 800-53 Rev.5

AU-11: Requires audit record retention.

MP-6: Defines media sanitization procedures.

SI-12: Addresses data retention limits and enforcement.

EU GDPR

Article 5(1)(e): Data must be kept no longer than necessary.

Article 17: Establishes the right to erasure ("right to be forgotten") when data is no longer lawfully retained.

EU NIS2

Article 21(2)(a): Requires risk-appropriate organizational policies, including information lifecycle management.

EU DORA

Article 5(1): ICT risk management includes data availability and removal when no longer required.

COBIT 2019

BAI03.04: Requires information lifecycle controls.

DSS01.06: Includes secure disposal procedures as part of safeguarding information assets.