					Insert Registered Legal Entity Name Here							
Document number: PII10					Document Title: **PII Retention, Deletion 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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Documented retention evidence and operational control
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Joint responsibility and processing records
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Erasure execution support
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Retention, deletion and disposal
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Customer instructions and processor records
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Deletion support and disposal capability
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Media disposal and backup handling
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Storage limitation and accountability
GDPR	Article 17	Controller	Supporting	Erasure execution support
GDPR	Article 24	Controller	Supporting	Controller measures
GDPR	Article 26	Joint Controller	Supporting	Joint responsibility allocation
GDPR	Article 28	Processor	Supporting	Processor deletion and return
GDPR	Article 30	Both	Supporting	Processing records
GDPR	Article 32	Both	Supporting	Secure processing and disposal support

ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimization, retention limitation and accountability
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Retention and temporary-file erasure controls
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Both	Primary	Deletion framework and documentation
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Deletion periods and deletion rules
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Both	Primary	Implementation and exceptions
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Responsibilities and implementation governance
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Privacy risk integration
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Secure disposal and information deletion

1. Scope

1.1 This policy establishes the organization's requirements for defining, reviewing, executing and evidencing retention, deletion, anonymization, de-identification, return, transfer and disposal of PII.

1.2 This policy applies to PII processed in controller, joint controller, processor and subprocessor contexts, including PII held in live systems, archives, backup copies, replicas, logs, staging environments, temporary files, paper records and storage media.

1.3 This policy applies to retention and deletion obligations arising from approved processing purposes, lawful basis records, controller instructions, contractual requirements, PII principal erasure outcomes, service exit, storage media disposal and PIMS monitoring findings.

1.4 This policy does not define lawful basis selection, privacy notice content, full PII principal rights handling, processor lifecycle governance, international transfer mechanisms, security control architecture, incident response workflow or PIMS audit methodology. Those controls are addressed in related policies.

1.5 For this policy, a material change means any change to processing purpose, PII category, PII principal category, system storage location, retention law or contract, customer instruction, backup architecture, archive approach, disposal method, processor or subprocessor arrangement, erasure workflow, or PIMS certification scope that affects retention, deletion or disposal.

2. Purpose

2.1 The purpose of this policy is to ensure that PII is retained only for approved purposes and periods, deleted or otherwise disposed of when no longer required, and supported by audit-ready evidence.

2.2 This policy enables the organization to demonstrate storage limitation, accountable retention governance, controlled deletion execution, secure disposal, processor instruction alignment, exception control and continual improvement without creating a separate deletion register.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define retention rule ownership and required retention metadata;

3.1.2 ensure retention rules are recorded in the PII Processing Inventory / ROPA;

3.1.3 ensure processor and subprocessor deletion actions are based on customer instruction or contract;

3.1.4 ensure expired PII is deleted, returned, transferred, anonymized, de-identified or disposed of using approved methods;

3.1.5 distinguish live systems, archives, backups, replicas, logs, staging areas and temporary files;

3.1.6 ensure deletion and disposal evidence is retained in canonical PIMS evidence objects;

3.1.7 ensure retention exceptions are time-bound, approved and reviewed;

3.1.8 integrate retention and deletion monitoring with nonconformity, corrective action and improvement.

4. Policy Statements

4.1 Retention rule assignment

4.1.1 [Controller] The Process Owner / Business Owner MUST assign a documented retention rule to each controller processing activity in REG02 before the processing activity begins.

4.1.2 [Joint Controller] The Process Owner / Business Owner MUST record joint-controller retention and deletion responsibility allocation in REG02 and REG08 before joint processing begins or changes.

4.1.3 [Processor] The Vendor / Procurement Owner MUST record customer retention, return, transfer or deletion instructions for processor activities in REG08 before processor processing begins or changes.

4.1.4 [Subprocessor] The Vendor / Procurement Owner MUST record subprocessor retention, return, transfer or deletion flow-down requirements in REG08 before subprocessor onboarding or instruction change.

4.1.5 [Both] The Privacy Lead / PIMS Manager MUST verify that each approved retention rule in REG02 includes the retention period, start trigger, owner, justification, final disposition and next review date before the rule is approved.

4.1.6 [Both] The Data Protection Officer / Privacy Advisor MUST record advice in REG02 or REG12 before approval of any retention rule involving legal conflict, high-risk processing, special-category PII, or retention beyond the original processing purpose.

4.2 Retention review and limitation

4.2.1 [Both] The Process Owner / Business Owner MUST review assigned retention rules in REG02 at least annually and within 30 days of a material change.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST approve or reject new or changed retention rules in REG02 within 10 business days of submission.

4.2.3 [Both] The System Owner / Application Owner MUST confirm the technical or manual enforcement method for each retention rule in REG02 before production go-live and during each annual retention review.

4.2.4 [Controller] The Process Owner / Business Owner MUST restrict active use of PII retained only for legal, contractual, audit or dispute reasons in REG02 within five business days of identifying the restriction condition.

4.2.5 [Both] The Privacy Lead / PIMS Manager MUST record unresolved over-retention risk or overdue retention review in REG12 within five business days of identification.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Exceptions

9.1.1 [All] The Process Owner / Business Owner MUST submit any request to retain PII beyond the approved REG02 retention rule in REG12 before the exception becomes active.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST approve or reject retention exception requests in REG12 before the exception becomes active.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of any exception involving legal conflict, erasure refusal, high-risk PII, external sharing or certification impact.

9.1.4 [All] Top Management MUST approve retention exceptions exceeding 90 days, affecting high-risk processing or affecting external assurance in REG12 before the exception becomes active.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST assign an owner, expiry date, compensating control and review frequency in REG12 for every approved retention, deletion or disposal exception.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST review each open exception in REG12 at least monthly until closure.

9.1.7 [All] The Process Owner / Business Owner MUST close or renew each exception in REG12 before the exception expiry date.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record a nonconformity in REG12 within five business days of identifying missing retention metadata, overdue retention review, unsupported retention, missed final disposition action or missing evidence.

10.1.2 [All] The System Owner / Application Owner MUST suspend new production use of a processing activity in REG12 when required technical retention controls are absent before go-live.

10.1.3 [All] The Process Owner / Business Owner MUST stop non-approved active use of PII retained only for legal, contractual, audit or dispute reasons within five business days and record the action in REG02 or REG12.

10.1.4 [Processor] The Vendor / Procurement Owner MUST escalate overdue customer-directed final disposition actions in REG08 and REG12 within five business days of missed contractual deadline.

10.1.5 [Subprocessor] The Vendor / Procurement Owner MUST escalate missing subprocessor final disposition evidence in REG08 and REG12 within five business days of missed contractual evidence deadline.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verify corrective action effectiveness for retention, deletion and disposal nonconformities in REG12 at the next scheduled audit or within 60 days of closure, whichever occurs first.

10.1.7 [Conditional] The Incident Response Coordinator MUST initiate REG10 handling when a retention, deletion or disposal nonconformity indicates a suspected PII incident.

11. Review and Maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy annually and record the review outcome in REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST review this policy within 30 days of material change to retention law, processing purpose, processor instruction, system architecture, backup architecture, archive approach, erasure workflow, disposal process or PIMS certification requirements.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST review privacy-significant changes to this policy in REG12 before approval.

11.1.4 [All] Top Management MUST approve material changes to this policy in REG12 before publication.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST record communication of approved policy changes in REG11 within 30 days of publication.

12. Related Policies

12.1 This policy is supported by the following related policies:

12.2 PII01 - Privacy Information Management System Policy

12.3 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.4 PII03 - PII Processing Inventory and Lawful Basis Policy

12.5 PII04 - Privacy Notice and Transparency Policy

12.6 PII06 - PII Principal Rights Management Policy

12.7 PII08 - Privacy by Design and Default Policy

12.8 PII09 - PII Collection, Use, Disclosure and Sharing Policy

12.9 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.10 PII14 - PII Security and Access Control Policy

12.11 PII15 - PII Incident and Breach Management Policy

12.12 PII17 - PIMS Documented Information and Evidence Management Policy

12.13 PII18 - PIMS Monitoring, Audit and Improvement Policy

13. Reference Standards and Frameworks

13.1 This policy is mapped to the following standards and regulations. The mapping explains how the policy supports the cited requirements and identifies the internal clauses that implement or support them.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapped to documented retention evidence, operational planning, retention metadata, implementation evidence and lifecycle execution records. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mapped to monitoring, metrics, overdue action review, nonconformity and corrective action for retention, deletion and disposal controls. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Mapped to joint-controller responsibility evidence and controller processing records containing retention and final disposition metadata. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].

13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Mapped to erasure execution support, deletion assessment routing and third-party evidence linkage where erasure outcomes require action. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Mapped to deletion or de-identification at end of processing, temporary-file handling, retention limitation and documented final disposition controls. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapped to processor customer agreements, documented customer purposes and processor processing records. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].

13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Mapped to processor support for customer obligations, temporary-file handling, and return, transfer or final disposition capability. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Mapped to storage media lifecycle handling, equipment reuse or release checks, and backup handling for PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Mapped to storage limitation, retention accountability, approved retention metadata, evidence and review. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Mapped to approved erasure outcome routing, execution evidence and incident escalation where erasure control failures indicate a suspected PII incident. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Mapped to controller governance, accountability measures, reviews, exceptions, corrective action and policy maintenance. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Mapped to joint-controller retention and deletion responsibility allocation. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Mapped to processor and subprocessor instruction alignment, return, transfer, final disposition, evidence and escalation. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Mapped to retention and final disposition metadata in processing records for controller and processor activities. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Mapped to secure operational handling of retained PII, technical enforcement, storage media control, backup handling and incident escalation. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Mapped to data minimization, use and retention limitation, final disposition when no longer required, restriction of retained PII and accountability evidence. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Mapped to time-limited retention, final disposition, automated or manual enforcement, and temporary-file handling. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Mapped to deletion framework governance, PII grouping, retention and deletion periods, archives and backup distinction, deletion-rule structure and documented procedure requirements. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Mapped to regular deletion period specification, standard deletion period identification and allocation of deletion rules to PII processing activities. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Mapped to implementation requirements for systems, manual processes, organization-wide aspects, processors, recovery handling and exception management. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Mapped to role assignment, documentation, operational embedding, audit and implementation governance for retention, deletion and disposal. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapped to risk-based privacy governance, leadership awareness, integration of privacy risk into the PIMS and retention-related risk context. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Mapped to information deletion, controlled lifecycle completion, storage media release and evidence of final disposition. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].