					Insert Registered Legal Entity Name Here							
Document number: PII03					Document Title: **PII Processing Inventory and Lawful Basis 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 4.1	Both	Supporting	PIMS role determination for processing activities
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Privacy risk assessment trigger linkage
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Control applicability and SoA linkage
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Processing inventory documented information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operational planning and control for processing records
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Operational privacy risk assessment linkage
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Inventory monitoring and measurement
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Inventory nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Controller purpose identification
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Controller lawful basis identification
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	DPIA screening linkage
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Joint controller processing responsibility records
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Controller records related to PII processing
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Processor customer

				agreement and instruction records
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Processor purpose alignment with customer instructions
ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Processor records related to PII processing
GDPR	Article 5(1)(a)	Controller	Supporting	Lawfulness, fairness and transparency linkage
GDPR	Article 5(1)(b)	Controller	Supporting	Purpose limitation
GDPR	Article 5(1)(c)	Controller	Supporting	Data minimization
GDPR	Article 5(1)(e)	Controller	Supporting	Storage limitation linkage
GDPR	Article 5(2)	Controller	Supporting	Accountability evidence
GDPR	Article 6	Controller	Primary	Lawfulness of processing
GDPR	Article 9	Conditional	Supporting	Special category processing condition
GDPR	Article 10	Conditional	Supporting	Criminal conviction and offence data condition
GDPR	Article 24	Controller	Supporting	Controller responsibility and measures
GDPR	Article 26	Joint Controller	Supporting	Joint controller arrangement records
GDPR	Article 28	Both	Supporting	Processor instruction and agreement records
GDPR	Article 30	Both	Primary	Records of processing activities
GDPR	Article 35	Controller	Supporting	DPIA screening linkage
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Purpose legitimacy and specification

ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Collection limitation
ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Data minimization
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Use, retention and disclosure limitation
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Accountability
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	PII protection purpose, collection, minimization, use, retention and disclosure controls
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	PIA benefit and trigger linkage

1. Scope

1.1 This policy defines the requirements for maintaining the PII Processing Inventory / ROPA and documenting lawful basis, processing purposes, processing roles, PII categories, PII principal categories, recipients, retention references, transfer references, processor instructions, joint controller records, and privacy risk screening linkage.

1.2 This policy applies to:

1.2.1 all PII processing activities within the PIMS scope;

1.2.2 processing performed as a controller, joint controller, processor, or subprocessor;

1.2.3 processing performed by business processes, systems, applications, suppliers, processors, subprocessors, and data-sharing recipients;

1.2.4 new processing, materially changed processing, and retired processing;

1.2.5 evidence maintained in REG02 and supporting evidence in REG01, REG03, REG04, REG05, REG07, REG08, REG09, and REG12.

1.3 This policy does not replace detailed privacy notice controls, consent controls, DPIA methodology, retention execution, international transfer mechanism selection, processor contracting controls, PII security controls, or documented information controls. Those requirements are defined in the related policies listed in Section 12.

1.4 For this policy, a processing inventory record means a REG02 entry describing a distinct PII processing activity, including its purpose, role, owner, PII categories, PII principal categories, lawful basis or customer instruction reference, systems, recipients, retention reference, transfer reference, privacy risk status, and review status.

1.5 For this policy, a material processing change means any change to processing purpose, lawful basis, PIMS role, PII category, PII principal category, recipient, system, supplier, subprocessor, processing location, transfer, retention rule, security classification, privacy notice, consent dependency, DPIA status, customer instruction, or certification scope.

2. Purpose

2.1 The purpose of this policy is to ensure that the organization can identify, document, justify, review, and demonstrate the PII processing activities within the PIMS scope.

2.2 This policy enables the organization to maintain a complete, current, and audit-ready PII processing inventory that supports lawful processing, accountability, privacy notices, consent management, privacy risk assessment, DPIA screening, retention, transfer governance, processor governance, and PIMS monitoring.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 establish REG02 as the authoritative PII processing inventory and ROPA evidence object;

3.1.2 ensure that each PII processing activity has an accountable owner;

3.1.3 distinguish controller, joint controller, processor, and subprocessor processing records;

3.1.4 document specific processing purposes before processing begins;

3.1.5 document lawful basis for controller processing before processing begins;

3.1.6 document customer instructions for processor and subprocessor processing before processing begins;

3.1.7 document PII categories, PII principal categories, recipients, retention references, transfer references, systems, and supplier relationships;

3.1.8 link inventory records to privacy notice, consent, DPIA, risk, supplier, transfer, control, and audit evidence where applicable;

3.1.9 ensure processing inventory records are reviewed, updated, and corrected when processing changes;

3.1.10 avoid creating separate lawful basis or processing inventory registers outside REG02.

4. Policy Statements

4.1 Processing inventory baseline

4.1.1 [Both] The Process Owner / Business Owner MUST create a REG02 processing inventory record before any new PII processing activity begins.

4.1.2 [Both] The Process Owner / Business Owner MUST record the required REG02 fields for each processing activity before the activity begins.

4.1.3 [Both] The Privacy Lead / PIMS Manager MUST approve the required REG02 field set in REG12 before initial PIMS operation and annually thereafter.

4.1.4 [Both] The Process Owner / Business Owner MUST classify the organization's PIMS role for each processing activity in REG02 before the activity begins.

4.1.5 [Both] The System Owner / Application Owner MUST link each system or application processing PII to the relevant REG02 processing activity before system go-live.

4.1.6 [Both] The Vendor / Procurement Owner MUST link each processor, subprocessor, third-party sharing, or joint controller relationship in REG08 to the relevant REG02 processing activity before agreement approval or onboarding.

4.2 Controller purpose and lawful basis records

4.2.1 [Controller] The Process Owner / Business Owner MUST document the specific processing purpose in REG02 before PII is collected, used, disclosed, or otherwise processed.

4.2.2 [Controller] The Privacy Lead / PIMS Manager MUST validate the lawful basis recorded in REG02 before controller processing begins and before any purpose change takes effect.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of a new lawful basis for high-risk processing, special category PII, criminal conviction or offence data, or materially changed controller processing.

4.2.4 [Controller] The Process Owner / Business Owner MUST link REG02 to REG05 before controller processing relies on consent as a lawful basis.

4.2.5 [Controller] The Process Owner / Business Owner MUST record the legitimate-interest assessment reference in REG04 before controller processing relies on legitimate interests.

4.2.6 [Conditional] The Process Owner / Business Owner MUST record the special category processing condition in REG02 before processing special category PII.

4.2.7 [Conditional] The Privacy Lead / PIMS Manager MUST record the criminal conviction or offence data authorization basis in REG02 before processing criminal conviction or offence data.

4.2.8 [Controller] The Process Owner / Business Owner MUST document purpose compatibility and privacy risk screening in REG02 and REG04 before using PII for a new purpose not previously recorded.

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

9. Exceptions

9.1 Processing inventory and lawful basis exceptions

9.1.1 [All] The Process Owner / Business Owner MUST request an exception in REG12 before operating a PII processing activity without a required REG02 field, lawful basis record, customer instruction reference, or review status.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST assess the privacy, certification, and operational impact of each processing inventory exception in REG12 within 10 business days of request.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of any exception involving lawful basis, special category PII, criminal conviction or offence data, high-risk processing, international transfer linkage, or customer instruction limitation.

9.1.4 [All] Top Management MUST approve processing inventory exceptions exceeding 30 days, affecting high-risk processing, or affecting certification scope in REG12 before the exception takes effect.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST set an expiry date not exceeding 90 days in REG12 for each approved processing inventory exception before approval.

9.1.6 [All] The Process Owner / Business Owner MUST close or reassess each processing inventory exception in REG12 within five business days of expiry.

10. Enforcement

10.1 Processing inventory and lawful basis enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record missing, inaccurate, outdated, or unapproved REG02 processing inventory evidence as a nonconformity in REG12 within five business days of identification.

10.1.2 [Controller] The Process Owner / Business Owner MUST suspend new controller processing when the required purpose or lawful basis evidence is missing from REG02 before launch.

10.1.3 [Processor] The Process Owner / Business Owner MUST suspend new processor processing when required customer instruction evidence is missing from REG02 or REG08 before service onboarding.

10.1.4 [Both] The System Owner / Application Owner MUST block system go-live for PII processing when required REG02 inventory linkage is missing before go-live approval.

10.1.5 [Both] The Vendor / Procurement Owner MUST block supplier, processor, subprocessor, third-party recipient, or joint controller onboarding when required REG02 and REG08 linkage evidence is missing before agreement approval.

10.1.6 [All] Top Management MUST review unresolved major processing inventory or lawful basis nonconformities in REG12 during management review.

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

11. Review and Maintenance

11.1 Policy review and maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy in REG12 annually and within 30 days of material change to processing inventory, lawful basis, processor instruction, ROPA, or certification requirements.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST review REG02 minimum field requirements in REG12 annually and within 30 days of material legal, regulatory, contractual, or processing change.

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 update REG03 and REG04 within 15 business days after approved policy changes that alter control applicability or privacy risk screening requirements.

11.1.6 [All] The Privacy Lead / PIMS Manager MUST record communication of approved changes to this policy 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 PII04 - Privacy Notice and Transparency Policy

12.5 PII05 - Consent and Preference Management Policy

12.6 PII07 - Privacy Risk Assessment and DPIA Policy

12.7 PII08 - Privacy by Design and Default Policy

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

12.9 PII10 - PII Retention, Deletion and Disposal Policy

12.10 PII11 - PII Accuracy and Quality Policy

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

12.12 PII13 - International PII Transfer Policy

12.13 PII14 - PII Security and Access Control Policy

12.14 PII17 - PIMS Documented Information and Evidence Management Policy

12.15 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 4.1** - Mapped to determining the organization's PIMS role for each processing activity and distinguishing controller, joint controller, processor, and subprocessor contexts. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].

13.2.2 **Clause 6.1.2** - Mapped to privacy risk assessment trigger linkage for new and materially changed PII processing activities. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].

13.2.3 **Clause 6.1.3** - Mapped to linking processing activities to control applicability and PIMS Statement of Applicability evidence. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].

13.2.4 **Clause 7.5** - Mapped to maintaining processing inventory, lawful basis, processor instruction, review, exception, and corrective action records as controlled documented information. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].

13.2.5 **Clause 8.1** - Mapped to operational planning and control for creating, validating, updating, reviewing, and retiring processing inventory records before processing begins or changes. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].

13.2.6 **Clause 8.2** - Mapped to operational privacy risk assessment linkage from processing inventory records and material processing change triggers. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.2.7 **Clause 9.1** - Mapped to monitoring and measuring processing inventory completeness, lawful basis validation, instruction linkage, review status, DPIA screening linkage, and reconciliation exceptions. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.8 **Clause 10.2** - Mapped to handling inventory and lawful basis nonconformities, exceptions, corrective actions, enforcement, and effectiveness verification. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].

13.2.9 **Annex A.1.2.2** - Mapped to identifying and documenting controller processing purposes before PII is collected, used, disclosed, or otherwise processed. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].

13.2.10 **Annex A.1.2.3** - Mapped to determining, documenting, validating, and demonstrating lawful basis for controller processing. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].

13.2.11 **Annex A.1.2.6** - Mapped to screening new and materially changed controller processing activities for DPIA need. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].

13.2.12 **Annex A.1.2.8** - Mapped to recording joint controller processing purposes and responsibility allocation references. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.2.13 **Annex A.1.2.9** - Mapped to maintaining controller records related to PII processing, including purposes, categories, recipients, retention references, transfers, lawful basis, risk screening, owner, status, and review evidence. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].

13.2.14 **Annex A.2.2.2** - Mapped to processor customer agreement and documented instruction evidence, including subject matter, duration, purpose, PII categories, and PII principal categories. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].

13.2.15 **Annex A.2.2.3** - Mapped to ensuring processor processing purposes remain aligned with documented customer instructions. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].

13.2.16 **Annex A.2.2.7** - Mapped to maintaining processor records related to processing PII on behalf of customers. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(a)** - Mapped to controller processing purpose, lawful basis validation, and accountability evidence before processing begins. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].

13.3.2 **Article 5(1)(b)** - Mapped to purpose specification, purpose compatibility assessment, and preventing undocumented new-purpose processing. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].

13.3.3 **Article 5(1)(c)** - Mapped to recording PII categories, PII principal categories, and source data before processing to support minimization review. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.3.4 **Article 5(1)(e)** - Mapped to recording retention rule or retention reference for each processing activity. Addressed by clauses [4.4.4; 8.1.6].

13.3.5 **Article 5(2)** - Mapped to accountability evidence for processing inventory, lawful basis validation, review, reconciliation, audit sampling, and corrective action. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].

13.3.6 Article 6 - Mapped to documenting and validating lawful basis for controller processing, including consent linkage, legitimate-interest assessment reference, and purpose compatibility. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].

13.3.7 Article 9 - Mapped to recording special category processing condition and privacy advice before special category PII processing. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].

13.3.8 **Article 10** - Mapped to recording the authorization basis for criminal conviction or offence data before processing. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].

13.3.9 **Article 24** - Mapped to controller governance, review, accountability, and management oversight of processing inventory and lawful basis records. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].

13.3.10 **Article 26** - Mapped to joint controller processing purpose and responsibility allocation evidence. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.3.11 **Article 28** - Mapped to processor and subprocessor instruction, agreement, relationship linkage, and onboarding controls. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].

13.3.12 **Article 30** - Mapped to controller and processor records of processing activities, including processing purposes, PII categories, PII principal categories, recipients, transfers, retention references, and customer instruction records. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].

13.3.13 **Article 35** - Mapped to DPIA screening linkage for new, materially changed, or high-risk controller processing activities. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3** - Mapped to purpose legitimacy, purpose specification, lawful basis linkage, and purpose compatibility evidence. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].

13.4.2 **Clause 5.4** - Mapped to collection limitation through documenting PII categories, PII principal categories, sources, and justification before processing begins. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.4.3 **Clause 5.5** - Mapped to data minimization through inventory field requirements, category documentation, recipient documentation, and review of current processing records. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].

13.4.4 **Clause 5.6** - Mapped to use, retention, disclosure, and transfer limitation through documented purposes, recipient categories, retention references, transfer linkage, and purpose change controls. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].

13.4.5 **Clause 5.10** - Mapped to accountability through ownership, inventory governance, review, reconciliation, audit sampling, exception handling, and corrective action evidence. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mapped to PII protection controls for purpose legitimacy, collection limitation, data minimization, and use, retention, and disclosure limitation. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Mapped to using processing inventory changes to trigger privacy risk assessment and DPIA screening before new or materially changed processing proceeds. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].