					Insert Registered Legal Entity Name Here							
Document number: PII09					Document Title: **PII Collection, Use, Disclosure and Sharing 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 operational control
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring and corrective action
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Purpose and processing records
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Lawful basis linkage
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Joint-controller sharing responsibilities
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Collection, processing and minimization limits
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Transfer routing linkage
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Transfer and disclosure records
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Processor instruction and records
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Processor transfer routing linkage
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Processor disclosure records and requests
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Purpose limitation, minimization and accountability
GDPR	Article 6	Controller	Referenced	Lawful basis linkage
GDPR	Article 24	Controller	Supporting	Controller responsibility
GDPR	Article 26	Joint Controller	Supporting	Joint-controller arrangements
GDPR	Article 28	Both	Supporting	Processor instructions and disclosure limits
GDPR	Article 30	Both	Supporting	Processing and recipient records

ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Purpose, collection, minimization and disclosure limitation
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Accountability and privacy compliance
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Purpose, collection, minimization, use and disclosure controls

1. Scope

1.1 This policy defines requirements for collecting, using, disclosing and sharing PII within the PIMS scope.

1.2 This policy applies to:

1.2.1 PII collection through direct, indirect, automated, manual, internal, external and third-party channels;

1.2.2 approved internal use of PII by business processes, systems and applications;

1.2.3 secondary use of PII for a new or materially changed purpose;

1.2.4 external disclosure of PII to recipients, partners, authorities, processors, subprocessors, suppliers and other third parties;

1.2.5 recurring data-sharing arrangements and one-off disclosures;

1.2.6 controller, joint controller, processor and subprocessor contexts;

1.2.7 REG02 - PII Processing Inventory / ROPA, REG08 - Processor, Subprocessor and Data Sharing Register, REG09 - International Transfer Register, and REG12 - Audit, Nonconformity, Corrective Action and Improvement Register.

1.3 This policy does not replace:

1.3.1 PII03 for processing inventory, lawful basis and ROPA ownership;

1.3.2 PII04 for privacy notice content, publication and version control;

1.3.3 PII05 for consent and preference operation;

1.3.4 PII06 for PII principal rights request handling;

1.3.5 PII07 for DPIA methodology and privacy risk assessment;

1.3.6 PII08 for privacy-by-design gates;

1.3.7 PII10 for retention, deletion and disposal execution;

1.3.8 PII11 for accuracy and quality management;

1.3.9 PII12 for processor, subprocessor and third-party lifecycle governance;

1.3.10 PII13 for international transfer mechanism selection and transfer risk controls;

1.3.11 PII14 for PII security and access control;

1.3.12 PII15 for incident and breach handling;

1.3.13 PII18 for PIMS-wide monitoring, audit, nonconformity, corrective action and improvement governance.

1.4 For this policy:

1.4.1 "approved use" means a use of PII that is recorded in REG02 for a specific processing activity, purpose, PII category, PII principal category, business owner and applicable PIMS role.

1.4.2 "collection" means obtaining PII directly from a PII principal, indirectly from another party, automatically from a system or device, or through an internal or external data source.

1.4.3 "secondary use" means using PII for a purpose that is not already recorded as an approved purpose in REG02 for the relevant processing activity.

1.4.4 "compatibility check" means a documented assessment in REG02 of the original purpose, proposed purpose, lawful-basis dependency, PII categories, PII principal expectations, minimization rationale, disclosure or transfer impact, and routing to other PIMS policies where needed.

1.4.5 "external disclosure" means making PII available to a party outside the organization or outside the documented customer instruction chain.

1.4.6 "data sharing" means a recurring or structured arrangement under which PII is disclosed, transferred, accessed, exchanged or made available to another party.

1.4.7 "sensitive recurring sharing" means recurring sharing involving special category PII, criminal offence PII, child PII, high-impact records, large-scale sharing, or external sharing involving a transfer location recorded in REG09.

2. Purpose

2.1 The purpose of this policy is to ensure that PII is collected, used, disclosed and shared only for documented, approved, limited and accountable purposes.

2.2 This policy enables the organization to demonstrate that collection and use are linked to REG02 processing records, that disclosures and data-sharing arrangements are recorded in REG08, that international transfer routing is linked to REG09, and that exceptions and nonconformities are handled through REG12.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 limit collection to PII that is necessary for documented purposes;

3.1.2 ensure internal use of PII is approved before processing begins;

3.1.3 require compatibility checks before secondary use;

3.1.4 require approval and evidence before external disclosure;

3.1.5 maintain data-sharing evidence in REG08 without creating a separate data-sharing register;

3.1.6 route international transfer dependencies to REG09 and PII13 without duplicating transfer mechanism controls;

3.1.7 define recurring sharing review cadence;

3.1.8 maintain audit-ready evidence for collection, use, disclosure, sharing, exceptions and corrective actions.

4. Policy Statements

4.1 Collection limitation

4.1.1 [Controller] The Process Owner / Business Owner MUST record the collection purpose, source or channel, PII categories, PII principal categories and minimum data elements in REG02 before any new collection activity or material collection change begins.

4.1.2 [Controller] The Privacy Lead / PIMS Manager MUST review the REG02 collection record before collection begins when a new PII category, source, channel or purpose is added.

4.1.3 [Controller] The Process Owner / Business Owner MUST record a necessity justification in REG02 for each PII data element before that element is collected.

4.1.4 [Processor] The Process Owner / Business Owner MUST record the customer instruction reference from REG08 in REG02 before collecting PII on behalf of a customer.

4.1.5 [Joint Controller] The Process Owner / Business Owner MUST record the joint-controller collection responsibility allocation in REG08 before joint collection begins.

4.2 Approved internal use controls

4.2.1 [Controller] The Process Owner / Business Owner MUST record approved internal use rules for each processing activity in REG02 before the use begins.

4.2.2 [Controller] The System Owner / Application Owner MUST implement only internal-use workflow fields, reports or exports that have a matching REG02 approved-use rule before production release.

4.2.3 [Processor] The Process Owner / Business Owner MUST record customer-instruction alignment in REG08 before using customer PII for any processor or subprocessor activity.

4.2.4 [Controller] The Privacy Lead / PIMS Manager MUST review approved-use rules in REG02 at least annually for each active processing activity.

4.2.5 [All] The Privacy Lead / PIMS Manager MUST record a nonconformity in REG12 within five business days when undocumented internal use of PII is identified.

[... 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 record an exception request in REG12 before deviating from an approved collection, use, disclosure or sharing rule.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST record an approval or rejection decision in REG12 before an exception is activated.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of an exception involving incompatible secondary use, sensitive recurring sharing, legally binding disclosure conflict or transfer routing.

9.1.4 [All] Top Management MUST record approval in REG12 before activation of any exception with a duration exceeding 30 calendar days or affecting more than one processing activity.

9.1.5 [All] The Process Owner / Business Owner MUST close an exception in REG12 by the expiry date or within five business days after the exception condition ends.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record unapproved collection, use, disclosure or sharing as a nonconformity in REG12 within five business days of identification.

10.1.2 [Controller] The Process Owner / Business Owner MUST suspend collection, use, disclosure or sharing within one business day when the Privacy Lead / PIMS Manager records absence of approved REG02 or REG08 evidence in REG12.

10.1.3 [Processor] The Process Owner / Business Owner MUST record a stop or escalation decision in REG08 and REG12 within one business day when customer PII is used or disclosed outside documented instruction.

10.1.4 [All] Top Management MUST review unresolved high-impact collection, use, disclosure or sharing nonconformities in REG12 within 30 calendar days of escalation.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST verify corrective action closure evidence in REG12 within 15 business days after the Privacy Lead / PIMS Manager marks closure.

11. Review and Maintenance

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

11.1.2 [All] The Privacy Lead / PIMS Manager MUST review this policy within 30 calendar days of a material change to PIMS scope, processing purposes, sharing model, transfer routing or applicable obligation and record the outcome in REG12.

11.1.3 [All] The Process Owner / Business Owner MUST recertify active REG02 and REG08 records at least annually and within 30 calendar days of a material processing change.

11.1.4 [All] The Internal Audit / Compliance Reviewer MUST include PII09 controls in annual audit sampling and record coverage in REG12.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST update related-policy references in REG12 within ten business days when PII03, PII08, PII10, PII12, PII13, PII14 or PII18 changes this policy's operating boundary.

12. Related Policies

12.1 This policy should be read with:

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 PII05 - Consent and Preference Management Policy

12.7 PII06 - PII Principal Rights Management Policy

12.8 PII07 - Privacy Risk Assessment and DPIA Policy

12.9 PII08 - Privacy by Design and Default Policy

12.10 PII10 - PII Retention, Deletion and Disposal Policy

12.11 PII11 - PII Accuracy and Quality Policy

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

12.13 PII13 - International PII Transfer Policy

12.14 PII14 - PII Security and Access Control Policy

12.15 PII15 - PII Incident and Breach Management Policy

12.16 PII17 - PIMS Documented Information and Evidence Management Policy

12.17 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 operational records and control over collection, approved use, secondary use, disclosure, sharing and transfer-routing evidence. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Mapped to monitoring, measurement, review, exception handling, nonconformity and corrective action for collection, use, disclosure and sharing controls. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Mapped to documented controller purposes, approved-use records and processing evidence in REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Mapped to lawful-basis linkage for collection, use and secondary-use routing without replacing PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Mapped to joint-controller collection and sharing responsibility evidence in REG08. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Mapped to collection limitation, processing limitation and minimization justification before PII is collected or used. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Mapped to transfer routing linkage through REG09 without replacing PII13 transfer mechanism controls. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Mapped to records of transfers, disclosures and recurring data-sharing arrangements in REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapped to processor customer-instruction alignment and processor records for collection, use and secondary-use limits. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Mapped to processor transfer routing linkage through REG09 without replacing PII13 transfer mechanism controls. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapped to processor disclosure records, disclosure-request notification status and disclosure authorization evidence in REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapped to purpose limitation, data minimization and accountability evidence for collection, use, secondary use, disclosure and sharing. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Mapped to lawful-basis linkage and routing for new or incompatible secondary use without replacing PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Mapped to controller governance, approvals, review and accountability measures for collection, use, disclosure and sharing. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Mapped to joint-controller collection and sharing responsibility evidence. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Mapped to processor and subprocessor instruction alignment, customer authorization and disclosure limits. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Mapped to processing, recipient, disclosure and sharing records in REG02 and REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapped to purpose specification, collection limitation, data minimization, use limitation and disclosure limitation. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Mapped to accountability, compliance evidence, review, exception management, audit sampling and corrective action. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mapped to purpose, collection limitation, minimization, use limitation, disclosure limitation and disclosure-record support. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].