					Insert Registered Legal Entity Name Here							
Document number: PII05					Document Title: **Consent and Preference Management 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 information and operational control for consent evidence
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, nonconformity, corrective action and improvement
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Lawful basis linkage
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Consent determination, obtaining and recording
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Controller processing records
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Processor agreements, customer purposes and processor records
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Processor support for controller obligations to PII principals
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Protection of PII processing records
GDPR	Article 4(11)	Controller	Supporting	Consent criteria
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Lawfulness, fairness, transparency and accountability
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Consent as lawful basis and changed-purpose linkage
GDPR	Article 7	Controller	Primary	Consent conditions and withdrawal
GDPR	Article 8	Conditional	Supporting	Child consent escalation

GDPR	Article 9(2)(a)	Conditional	Supporting	Explicit consent for special category processing
GDPR	Article 24	Controller	Supporting	Controller responsibility and measures
GDPR	Article 28	Both	Supporting	Processor instruction and assistance linkage
GDPR	Article 30	Both	Supporting	Processing records linkage
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Consent and choice, transparency and compliance principles
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Consent and choice controls
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Consent record and receipt structure where used

1. Scope

1.1 This policy defines mandatory requirements for determining when consent is required, requesting consent, capturing consent evidence, managing preferences, processing withdrawals, maintaining consent records, and reviewing consent mechanisms.

1.2 This policy applies to PII processing where consent is selected or required as a lawful basis, where explicit consent is required, where consent preferences are captured, or where the organization manages consent records on behalf of a controller.

1.3 This policy applies to controller, joint controller, processor, and subprocessor contexts.

1.4 Processor and subprocessor obligations apply only where consent records, preference states, or withdrawal instructions are managed under documented controller or customer instructions.

1.5 This policy does not make consent the default lawful basis for PII processing.

1.6 Lawful basis determination remains governed by PII03 - PII Processing Inventory and Lawful Basis Policy.

2. Purpose

2.1 The purpose of this policy is to ensure that consent and preference management is lawful, transparent, demonstrable, revocable, technically enforceable, and supported by controlled evidence.

2.2 This policy ensures that consent is requested only where appropriate, that consent records are complete and traceable, that withdrawals are honored, and that consent evidence remains available for audit, inquiry, and accountability purposes.

3. Objectives

3.1 The objectives of this policy are to ensure consent is used only when it is the appropriate lawful basis or when required for the processing activity.

3.2 The objectives of this policy are to ensure consent requests are specific, informed, distinguishable, and linked to the applicable privacy notice.

3.3 The objectives of this policy are to ensure consent and preference records are captured and maintained in REG05.

3.4 The objectives of this policy are to ensure withdrawal and preference changes are acted upon within defined operational timeframes.

3.5 The objectives of this policy are to ensure consent records are linked to processing purposes in REG02 and notice versions in REG07.

3.6 The objectives of this policy are to ensure processor and subprocessor consent-support activities follow documented controller or customer instructions.

3.7 The objectives of this policy are to ensure consent mechanisms are monitored, reviewed, corrected, and auditable.

4. Policy Statements

4.1 Consent Applicability and Lawful Basis

4.1.1 [Controller] The Process Owner / Business Owner MUST record in REG02 whether consent is required or selected before any new or materially changed PII processing activity that relies on consent begins.

4.1.2 [Controller] The Privacy Lead / PIMS Manager MUST verify in REG02 and REG05 that consent is not selected as the default lawful basis before approving a new or materially changed consent-based processing activity.

4.1.3 [Controller] The Data Protection Officer / Privacy Advisor MUST review the consent basis in REG04 before launch where the processing involves special categories of PII, child-facing services, high-risk processing, or an imbalance between the organization and the PII principal.

4.1.4 [Joint Controller] The Privacy Lead / PIMS Manager MUST document the party responsible for obtaining, recording, refreshing, and honoring consent in REG02 and REG05 before joint-controller processing begins.

4.1.5 [Processor] The Privacy Lead / PIMS Manager MUST record customer instructions for consent capture, preference management, or withdrawal support in REG08 and REG05 before implementing a consent mechanism on behalf of a controller.

4.1.6 [Subprocessor] The Vendor / Procurement Owner MUST record consent-related subprocessor obligations in REG08 before a subprocessor is permitted to handle consent records, preference states, or withdrawal instructions.

4.2 Consent Request and Capture

4.2.1 [Controller] The Process Owner / Business Owner MUST ensure each consent request is purpose-specific and linked to the applicable REG07 privacy notice version before the consent request is presented to a PII principal.

4.2.2 [Controller] The System Owner / Application Owner MUST configure consent mechanisms to require an affirmative action before processing begins where explicit or opt-in consent is required.

4.2.3 [Controller] The Process Owner / Business Owner MUST record the PII principal reference, purpose, PII category, consent wording or version, privacy notice version, capture channel, timestamp, method, status, and applicable validity period in REG05 when consent is captured.

4.2.4 [Conditional] The Privacy Lead / PIMS Manager MUST record age-assurance or authorization logic in REG05 and trigger REG04 review before launch where consent relates to child-facing processing.

4.2.5 [Conditional] The Privacy Lead / PIMS Manager MUST mark consent as explicit in REG05 before processing begins where explicit consent is required for the selected purpose.

4.2.6 [Both] The System Owner / Application Owner MUST prevent processing that relies on consent from proceeding before REG05 shows an active consent status for the relevant purpose.

[... 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 request an exception in REG12 before deviating from an approved consent capture, preference management, withdrawal, or evidence requirement.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST approve or reject each consent-related exception in REG12 before implementation and assign an expiry date and compensating control for any approved exception.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST review the exception in REG04 or REG12 before approval where the exception involves explicit consent, child-facing processing, high-risk processing, or a withdrawal mechanism.

9.1.4 [Both] The System Owner / Application Owner MUST block production release or disable the affected consent mechanism when an exception required by this policy has not been approved in REG12 before go-live.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record a consent-related nonconformity in REG12 within five business days of identifying missing, invalid, unlinked, or unreliable consent evidence.

10.1.2 [Controller] The Process Owner / Business Owner MUST suspend or remediate processing for the affected purpose before further consent-based processing continues where consent is required but cannot be demonstrated in REG05.

10.1.3 [Both] The System Owner / Application Owner MUST disable or correct a nonconforming consent capture, preference, or withdrawal mechanism within the timeframe assigned in REG12.

10.1.4 [Processor] The Vendor / Procurement Owner MUST escalate customer-instruction failures involving consent records, preference states, or withdrawal support in REG08 and REG12 within five business days of identification.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST verify closure evidence for consent-related corrective actions in REG12 by the assigned due date.

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 a material change to consent law, consent technology, preference-management tooling, privacy notice structure, 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 PII07 - Privacy Risk Assessment and DPIA Policy

12.8 PII08 - Privacy by Design and Default Policy

12.9 PII09 - PII Collection, Use, Disclosure and Sharing 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 PII14 - PII Security and Access Control Policy

12.14 PII16 - Privacy Training, Awareness and Competence Policy

12.15 PII17 - PIMS Documented Information and Evidence Management Policy

12.16 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 information and operational control for determining consent applicability, capturing consent evidence, managing withdrawal, versioning consent records, testing mechanisms, and maintaining REG05. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.2; 4.5.3; 4.5.4; 7.1.1; 7.1.2; 7.1.3; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mapped to consent monitoring, metrics, audit sampling, nonconformity recording, corrective action, and effectiveness verification. Addressed by clauses [4.5.5; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.2.3** - Mapped to confirming when consent is an appropriate lawful basis and linking consent records to REG02 lawful-basis records. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].

13.2.4 **Annex A.1.2.4; Annex A.1.2.5** - Mapped to determining when and how consent is obtained, capturing consent, recording proof, managing explicit consent, withdrawal, refresh, and consent status. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.5 **Annex A.1.2.9** - Mapped to controller records for consent-based processing, consent history, notice linkage, evidence retention, and audit-ready consent records. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapped to processor customer agreements, customer purpose and instruction alignment, and processor records where consent-support services are performed for a controller. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 8.1.4; 10.1.4].

13.2.7 **Annex A.2.3.2** - Mapped to processor support for controller obligations to PII principals where consent withdrawal, preference changes, or consent evidence are handled under customer instruction. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].

13.2.8 **Annex A.3.14** - Mapped to protection of consent and preference records against unauthorized alteration and to preservation of audit-trail evidence. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.3 GDPR

13.3.1 **Article 4(11)** - Mapped to consent criteria requiring consent to be specific, informed, affirmative where required, and linked to the relevant purpose and notice version. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].

13.3.2 **Article 5(1)(a); Article 5(2)** - Mapped to lawfulness, fairness, transparency, accountability evidence, audit sampling, corrective action, and proof of consent-based processing. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.5.3; 4.5.5; 8.1.1; 8.1.5; 10.1.1; 10.1.5].

13.3.3 **Article 6(1)(a); Article 6(4)** - Mapped to consent as a lawful basis for specific purposes and to reassessment or refreshed consent where purpose or processing conditions materially change. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

13.3.4 Article 7 - Mapped to demonstrability, distinguishable consent requests, withdrawal, ease of withdrawal, consent validity, and retained consent history. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.4; 4.4.5; 10.1.2].

13.3.5 Article 8 - Mapped to child-facing consent escalation, age-assurance or authorization logic, and privacy risk review before launch. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].

13.3.6 **Article 9(2)(a)** - Mapped to explicit consent handling where explicit consent is selected for special-category processing. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].

13.3.7 **Article 24** - Mapped to controller governance measures, review, approval, exceptions, corrective action, and management oversight for consent controls. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.2; 6.1.3; 9.1.1; 9.1.2; 11.1.1; 11.1.4].

13.3.8 **Article 28** - Mapped to processor instruction handling, consent-support evidence, withdrawal support, subprocessor obligations, and customer instruction escalation. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 10.1.4].

13.3.9 **Article 30** - Mapped to linking consent records to processing purposes, controller records, processor support records, and REG02/REG05 traceability. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Mapped to consent and choice, transparency and notice linkage, withdrawal, accountability, and privacy compliance evidence. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.5.3; 4.5.5; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3** - Mapped to consent and choice controls requiring meaningful, informed, unambiguous consent, preference modification, and timely processing changes following consent modification or withdrawal. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.6 ISO/IEC TS 27560:2023

13.6.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Mapped to consent record and receipt concepts, consent recordkeeping, consent record structure, consent status, notice version linkage, receipt structure, and consent receipt interpretation where such records or receipts are used. Addressed by clauses [4.2.3; 4.3.2; 4.3.6; 4.4.3; 4.4.4; 4.5.2; 4.5.3; 7.1.6].

13.7 Internal Requirements

13.7.1 Internal requirement - Clauses defining REG05 as the authoritative evidence object, non-standard evidence approval, operational release blocking, training, policy maintenance, and communication support implementation consistency but are not directly mapped to a single external clause. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].