					Insert Registered Legal Entity Name Here							
Document number: PII06					Document Title: **PII Principal Rights 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	Rights request 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.1.3.2	Controller	Primary	Obligations to PII principals
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Objection, access, correction and erasure
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Third-party notification and copy of PII processed
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Request handling and automated decision-making obligations
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Controller processing records
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Customer agreement, obligation support and processor records
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Processor support for PII principal obligations
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Protection of rights request records
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparency and accountability
GDPR	Article 11; Article 12	Controller	Primary	Identification, request modalities, timing and response governance
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Access, rectification and erasure

GDPR	Article 18; Article 19; Article 20	Controller	Primary	Restriction, notification and portability
GDPR	Article 21; Article 22	Controller	Primary	Objection and automated decision-making
GDPR	Article 24	Controller	Supporting	Controller responsibility and measures
GDPR	Article 26	Joint Controller	Supporting	Joint-controller rights allocation
GDPR	Article 28	Both	Primary	Processor assistance for rights requests
GDPR	Article 30	Both	Supporting	Processing records linkage
GDPR	Article 32	Both	Supporting	Secure handling of rights evidence and disclosures
GDPR	Article 39	Conditional	Supporting	DPO advice and monitoring where applicable
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Transparency, individual participation, accountability and compliance
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	PII principal participation and access

1. Scope

1.1 This policy defines mandatory requirements for receiving, validating, evaluating, fulfilling, refusing, extending, closing, monitoring and evidencing PII principal rights requests.

1.2 This policy applies to requests by PII principals or authorized representatives concerning access, rectification, erasure, restriction, portability, objection, automated decision-making, consent withdrawal routing, complaints, and related inquiries.

1.3 This policy applies to controller, joint controller, processor and subprocessor contexts. Processor and subprocessor obligations apply only where the organization supports a controller, customer or upstream processor under documented instructions.

1.4 This policy does not replace:

1.4.1 PII03 for processing inventory and lawful basis records;

1.4.2 PII04 for privacy notice content and publication;

1.4.3 PII05 for consent and preference fulfilment;

1.4.4 PII10 for retention, deletion and disposal execution;

1.4.5 PII11 for accuracy and quality governance;

1.4.6 PII12 for processor and subprocessor lifecycle governance;

1.4.7 PII15 for incident and breach handling.

2. Purpose

2.1 The purpose of this policy is to ensure that PII principal rights requests are handled consistently, lawfully, securely, within defined timeframes, and with audit-ready evidence.

2.2 This policy ensures that the organization can demonstrate accountability for request intake, identity verification, evaluation, fulfilment, refusal, extension, processor cooperation, closure and continual improvement.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 Provide consistent intake and tracking for all PII principal rights requests.

3.1.2 Verify requestor identity or authority before disclosure, correction, deletion, restriction or portability.

3.1.3 Evaluate requests against processing records, role classification, legal obligations, contractual obligations and technical feasibility.

3.1.4 Fulfil valid requests within documented deadlines.

3.1.5 Record refusal, partial fulfilment, extension and closure evidence.

3.1.6 Support controller obligations where the organization acts as processor or subprocessor.

3.1.7 Protect rights request records and response packages against unauthorized disclosure or alteration.

3.1.8 Monitor rights request performance and drive corrective action where required.

4. Policy Statements

4.1 Intake, Logging and Classification

4.1.1 [All] The Privacy Lead / PIMS Manager MUST record each PII principal rights request in REG06 within two business days of receipt.

4.1.2 [All] The Privacy Lead / PIMS Manager MUST classify each request type, request channel, request date, requestor identity reference, assigned owner, internal due date, statutory or contractual due date, and current status in REG06 before evaluation begins.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST acknowledge receipt or provide the next required communication to the requestor within five business days of intake and record the communication in REG06.

4.1.4 [Controller] The Process Owner / Business Owner MUST link each request to the relevant REG02 processing activity before fulfilment actions are assigned.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST identify the joint-controller party responsible for handling the request in REG02, REG06 or REG08 before substantive evaluation begins.

4.1.6 [Processor] The Privacy Lead / PIMS Manager MUST record each customer instruction relating to a PII principal rights request in REG06 and REG08 before support activity begins.

4.1.7 [Subprocessor] The Vendor / Procurement Owner MUST record each upstream instruction relating to a PII principal rights request in REG06 or REG08 before subprocessor support activity begins.

4.1.8 [All] The Incident Response Coordinator MUST record a REG10 escalation within one business day where a rights request indicates a possible PII incident or breach.

4.2 Identity Verification, Scope and Evaluation

4.2.1 [Controller] The Privacy Lead / PIMS Manager MUST verify the requestor's identity or representative authority in REG06 before disclosing PII or making a requested change.

4.2.2 [Controller] The Privacy Lead / PIMS Manager MUST request only the minimum additional information needed for verification and record the request in REG06 when identity or authority is insufficient.

4.2.3 [Controller] The Process Owner / Business Owner MUST identify relevant systems, records, purposes, PII categories, recipients and retention constraints from REG02 before evaluating fulfilment.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor MUST review high-risk, disputed, unclear, excessive, repeated, refused or partially fulfilled requests in REG06 before the decision is communicated.

4.2.5 [Controller] The System Owner / Application Owner MUST verify that proposed response extracts exclude unrelated PII and unauthorized third-party data before the response package is released.

4.2.6 [Controller] The Information Security Lead MUST review the response delivery method in REG06 or REG12 before high-volume, sensitive, special-category or high-risk PII is disclosed.

4.2.7 [Controller] The Data Protection Officer / Privacy Advisor MUST review automated decision-making or profiling-related requests in REG06 and REG04 before fulfilment, refusal or escalation.

4.2.8 [Both] The Privacy Lead / PIMS Manager MUST record the evaluation outcome, applicable request type, decision, rationale and next action in REG06 before fulfilment or refusal.

[... 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 approved rights intake, verification, fulfilment, response or closure requirements.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST approve or reject each rights-handling exception in REG12 before implementation.

9.1.3 [Controller] The Data Protection Officer / Privacy Advisor MUST review any exception involving refusal, partial fulfilment, identity uncertainty, sensitive PII, automated decision-making, child-related requests or high-risk processing before approval.

9.1.4 [Both] The System Owner / Application Owner MUST block disclosure, correction, deletion, restriction or export activity where a required exception has not been approved in REG12 before action.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST assign an expiry date, owner and compensating control for every approved rights-handling exception in REG12 before the exception becomes active.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record a nonconformity in REG12 within five business days of identifying an overdue, missing, incomplete, unverified or unsupported rights request record.

10.1.2 [Controller] The System Owner / Application Owner MUST suspend response disclosure until identity, authority and response-package checks are recorded in REG06.

10.1.3 [Both] The Vendor / Procurement Owner MUST escalate processor, subprocessor or third-party non-cooperation in REG08 and REG12 within five business days of identification.

10.1.4 [All] Top Management MUST assign corrective action ownership in REG12 when rights request failures are systemic, repeated or certification-relevant.

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

10.1.6 [All] The Incident Response Coordinator MUST initiate REG10 review within one business day where a rights request nonconformity indicates unauthorized disclosure, loss, alteration, unavailability or other 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 rights request law, processing activity scope, rights tooling, identity verification method, processor service model 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 PII05 - Consent and Preference 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 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 PII16 - Privacy Training, Awareness and Competence Policy

12.17 PII17 - PIMS Documented Information and Evidence Management Policy

12.18 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 rights request records, operational request workflow, identity verification, fulfilment, response, closure and processor-support evidence. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mapped to rights request metrics, overdue request monitoring, audit sampling, nonconformity recording, corrective action and effectiveness verification. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.3.2** - Mapped to determining and fulfilling obligations to PII principals through documented rights categories, intake channels, verification, evaluation, response and closure criteria. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].

13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Mapped to objection, access, correction, erasure, restriction handling, verification, fulfilment and disputed accuracy handling. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].

13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Mapped to third-party notification following rights outcomes and provision of copies or portable response packages. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].

13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Mapped to documented handling of legitimate requests, deadlines, extensions, refusal, closure and automated decision-making request review. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.7 **Annex A.1.2.9** - Mapped to linking rights requests to processing records, processing purposes, systems, categories, recipients and retention constraints. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].

13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapped to customer agreement instructions, processor support for customer obligations and processor records for rights-support activities. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].

13.2.9 **Annex A.2.3.2** - Mapped to processor means for supporting controller obligations to PII principals, including retrieval, correction, restriction, deletion and export support under documented instruction. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].

13.2.10 **Annex A.3.14** - Mapped to protection of rights request records, secure response package handling, response delivery checks and closure evidence protection. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(2)** - Mapped to transparent rights handling, accountability evidence, request logs, response records, audit sampling and corrective action. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].

13.3.2 **Article 11; Article 12** - Mapped to identification, additional information where necessary, response timing, communications, extension, refusal and request closure. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.3.3 **Article 15; Article 16; Article 17** - Mapped to access search results, rectification, erasure, verification, fulfilment evidence and response package delivery. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].

13.3.4 **Article 18; Article 19; Article 20** - Mapped to restriction, notification of rights outcomes to relevant parties, and portability or copy delivery. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].

13.3.5 **Article 21; Article 22** - Mapped to objection evaluation and automated decision-making or profiling request review. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].

13.3.6 **Article 24** - Mapped to controller governance measures, roles, workflow ownership, review, exceptions, corrective action and management oversight for rights handling. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Mapped to identifying joint-controller responsibility for handling requests before substantive evaluation begins. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Mapped to processor and subprocessor assistance, documented customer instructions, support deadlines, no direct response without authorization and escalation of non-cooperation. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Mapped to linking rights requests to processing records, processing activities, systems, PII categories, recipients and processor records. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Mapped to secure rights request handling, response delivery protection, unauthorized disclosure prevention and protection of rights evidence. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Mapped to Data Protection Officer / Privacy Advisor advice and monitoring for high-risk, disputed, refused, extended and automated decision-making-related rights requests. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Mapped to transparency of rights channels, individual participation and access, accountability, complaint/redress procedures, privacy compliance monitoring and audit evidence. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.10** - Mapped to PII principal participation and access, identity verification, access, rectification, deletion, status updates, processor support and complaint/redress mechanisms. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

13.6 Internal Requirements

13.6.1 Internal requirement - Clauses defining REG06 as the primary rights evidence object, training, non-standard workflow approval, exception expiry, policy review and policy change communication support implementation consistency but are not directly mapped to a single external clause. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].