					Insert Registered Legal Entity Name Here							
Document number: PII12					Document Title: **Processor, Subprocessor and Third-Party Privacy 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 4.1	Both	Supporting	PIMS role determination for third-party processing relationships
ISO/IEC 27701:2025	Clause 6.1.2; Clause 8.2	Both	Supporting	Privacy risk and due diligence linkage
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Documented processor relationship controls and operational control
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring and corrective action for processor relationships
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Primary	Contracts with PII processors
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Controller processor relationship records
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Customer agreement and documented instruction alignment
ISO/IEC 27701:2025	Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Infringing instruction, customer obligation support, and processor records
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Customer assistance for PII principal obligations
ISO/IEC 27701:2025	Annex A.2.4.3	Processor	Supporting	Return, transfer, or disposal of PII
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Third-party disclosure records and disclosure-request handling

ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Subcontractor disclosure, engagement, and change
GDPR	Article 5(2)	Controller	Supporting	Accountability evidence
GDPR	Article 24	Controller	Supporting	Controller measures for processor governance
GDPR	Article 26	Joint Controller	Referenced	Relationship classification and joint-controller linkage
GDPR	Article 28	Both	Primary	Processor and subprocessor governance
GDPR	Article 30	Both	Supporting	Processing relationship records
GDPR	Article 32	Both	Supporting	Security of processing linkage
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Accountability, information security, and privacy compliance
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	PII processor supplier relationship, monitoring, and change management
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23	Both	Supporting	Supplier, ICT supply chain, monitoring, and cloud service controls
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Conditional	Supporting	Cloud processor customer assistance and purpose limits
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Conditional	Supporting	Cloud disclosure notification, disclosure records, and subcontractor transparency

ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Conditional	Supporting	Cloud breach interface, exit, contract measures, subcontracts, and location
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Both	Supporting	Acquisition and supply relationship strategy
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Both	Primary	Supplier relationship planning, selection, agreement, management, and termination

1. Scope

1.1 This policy defines the privacy management requirements for processors, subprocessors, subcontracted PII processors, suppliers, service providers, cloud service providers, and other third parties that process, access, receive, store, transmit, support, or otherwise handle PII within the PIMS scope.

1.2 This policy applies to the following relationships and activities:

1.2.1 the organization acting as a PII controller using processors;

1.2.2 the organization acting as a joint controller where third-party role classification is required;

1.2.3 the organization acting as a PII processor using subprocessors or subcontractors;

1.2.4 the organization acting as a subprocessor receiving customer instructions;

1.2.5 third-party relationships that require privacy due diligence, contract controls, documented instructions, subprocessor approval, monitoring, assurance, incident interface, transfer linkage, return, deletion, or exit evidence.

1.3 This policy uses REG08 - Processor, Subprocessor and Data Sharing Register as the primary evidence object for processor, subprocessor, and third-party privacy management.

1.4 This policy relies on other PIMS policies for specialist controls:

1.4.1 PII03 governs processing inventory and lawful basis records in REG02.

1.4.2 PII06 governs PII principal rights request handling in REG06.

1.4.3 PII07 governs privacy risk assessment and DPIA handling in REG04.

1.4.4 PII09 governs collection, use, disclosure, and sharing rules.

1.4.5 PII10 governs retention, deletion, disposal, return, and disposal evidence.

1.4.6 PII13 governs international transfer mechanisms and transfer risk records in REG09.

1.4.7 PII14 governs PII security and access control requirements.

1.4.8 PII15 governs PII incident and breach management in REG10.

1.4.9 PII17 governs documented information and evidence control.

1.4.10 PII18 governs monitoring, audit, nonconformity, corrective action, and improvement in REG12.

1.5 For this policy:

1.5.1 "processor relationship" means a relationship where an external party processes PII on behalf of the organization as controller.

1.5.2 "subprocessor relationship" means a relationship where an external party processes PII on behalf of the organization when the organization is acting as processor or subprocessor.

1.5.3 "third-party privacy relationship" means a relationship with a third party that receives, accesses, supports, or affects PII processing and must be classified in REG08.

1.5.4 "material third-party privacy change" means a change to processing purpose, PII categories, PII principal categories, processing location, subprocessor, subcontractor, access method, security posture, customer instruction, contract terms, transfer location, incident interface, return/deletion capability, or assurance status.

1.5.5 "high-risk processor relationship" means a processor, subprocessor, or third-party relationship involving large-scale PII, special category PII, criminal-offence PII, vulnerable individuals, systematic monitoring, high business dependency, privileged access, external hosting, cross-border processing, unresolved due-diligence findings, or material customer assurance obligations.

2. Purpose

2.1 The purpose of this policy is to ensure that processors, subprocessors, and third parties handling PII are identified, assessed, approved, contracted, instructed, monitored, changed, and exited using consistent privacy governance controls and audit-ready evidence.

2.2 This policy supports accountability by ensuring that processor and subprocessor relationships are documented in REG08, linked to relevant processing records, risk records, transfer records, incident records, and corrective action records, and reviewed throughout the relationship lifecycle.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 ensure that processor, subprocessor, and third-party privacy relationships are identified before onboarding, renewal, or material change;

3.1.2 ensure that each relationship is classified by PIMS role and linked to the relevant PII processing inventory record;

3.1.3 ensure that privacy due diligence and security assurance are completed before approval;

3.1.4 ensure that written contracts, customer instructions, and flow-down obligations are documented before PII processing begins;

3.1.5 ensure that subprocessors are disclosed, approved, changed, and monitored according to contract requirements;

3.1.6 ensure that processor and subprocessor assistance for rights, DPIAs, security, audit, incident interface, return, deletion, transfer linkage, and exit is coordinated through existing PIMS policies and evidence objects;

3.1.7 ensure that high-risk processor and subprocessor relationships are monitored, reassessed, and corrected when control weaknesses are identified;

3.1.8 avoid duplicate registers by using REG08 as the single processor, subprocessor, and data sharing evidence object.

4. Policy Statements

4.1 Relationship identification and classification

4.1.1 [All] The Privacy Lead / PIMS Manager MUST define the minimum REG08 fields for processor, subprocessor, and third-party privacy relationship records before initial operation of this policy and annually thereafter, with review evidence retained in REG12.

4.1.2 [All] The Process Owner / Business Owner MUST identify each proposed third-party relationship that will process, access, receive, store, transmit, support, or otherwise affect PII in REG08 before procurement, onboarding, renewal, or material third-party privacy change.

4.1.3 [Both] The Privacy Lead / PIMS Manager MUST classify each third-party privacy relationship as controller, joint controller, processor, subprocessor, or other third-party relationship in REG08 before contract approval or before PII processing begins, whichever occurs first.

4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST review ambiguous, high-risk, or disputed relationship classifications in REG08 before approval and MUST retain advice evidence in REG12.

4.1.5 [All] The Vendor / Procurement Owner MUST block onboarding, renewal, or expansion of any third-party privacy relationship until REG08 is completed and linked to REG02, REG04, REG09, or REG10 where those evidence objects are triggered.

4.1.6 [All] The Vendor / Procurement Owner MUST record the relationship owner, service description, PII categories, PII principal categories, processing role, processing locations, subprocessor indicator, assurance status, and review date in REG08 before the relationship is approved.

4.2 Due diligence and risk assessment

4.2.1 [All] The Vendor / Procurement Owner MUST complete privacy due diligence evidence in REG08 before selecting, renewing, or materially changing any processor, subprocessor, or third-party relationship that processes or accesses PII.

4.2.2 [All] The Information Security Lead MUST review security assurance evidence for each processor, subprocessor, or third-party relationship with PII access or hosting before approval, and MUST record the outcome in REG08 or REG12.

4.2.3 [Both] The Privacy Lead / PIMS Manager MUST trigger privacy risk and DPIA screening in REG04 for high-risk processor relationships and material third-party privacy changes before approval, with the REG04 reference recorded in REG08.

4.2.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST provide advice in REG04 or REG12 before approval of a relationship involving high residual privacy risk, special category PII, large-scale processing, systematic monitoring, or unresolved role classification.

4.2.5 [All] The Vendor / Procurement Owner MUST record the due diligence decision as approved, conditionally approved, rejected, or deferred in REG08 before contract signature, renewal, or material change approval.

4.2.6 [All] The Vendor / Procurement Owner MUST reassess high-risk processor relationships at least annually and other active PII processor or subprocessor relationships at least every 24 months, with reassessment evidence recorded in REG08 and overdue actions recorded in REG12.

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

9. Exceptions

9.1 Exception handling

9.1.1 [All] The Vendor / Procurement Owner MUST submit an exception request in REG12 before any deviation from processor due diligence, contract evidence, assurance evidence, monitoring, subprocessor approval, or exit evidence requirements.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST assess the privacy impact of each requested exception in REG12 within five business days after submission and MUST link REG08, REG04, REG09, or REG10 where applicable.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST provide advice in REG12 before approval of any exception involving high-risk processing, missing processor contract terms, unapproved subprocessor use, unresolved customer instruction concerns, or material transfer linkage gaps.

9.1.4 [All] Top Management MUST approve exceptions in REG12 before processing proceeds when the exception affects high-risk processing, missing contract evidence, unresolved major due-diligence findings, missing incident interface, missing transfer linkage, or certification scope.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST assign an expiry date not exceeding 90 days and compensating controls in REG12 before any exception becomes effective.

9.1.6 [All] The Vendor / Procurement Owner MUST reassess, close, or escalate each processor and subprocessor exception in REG12 within five business days after expiry.

10. Enforcement

10.1 Enforcement actions

10.1.1 [All] The Vendor / Procurement Owner MUST block onboarding, renewal, expansion, or continued use of a processor, subprocessor, or third party when required REG08 due diligence,

contract, approval, or monitoring evidence is missing before PII processing begins or continues.

10.1.2 [All] The Process Owner / Business Owner MUST suspend new PII sharing or processing expansion with an unapproved processor, subprocessor, or third party until REG08 approval evidence is complete.

10.1.3 [Both] The Incident Response Coordinator MUST escalate missed supplier incident notice obligations or late supplier incident notices to REG10 and REG12 within one business day after identification.

10.1.4 [All] The Privacy Lead / PIMS Manager MUST open a nonconformity in REG12 within five business days after identifying unauthorized processor use, unauthorized subprocessor use, missing contract evidence, repeated overdue monitoring, or failed exit evidence.

10.1.5 [All] Top Management MUST review unresolved major processor, subprocessor, or third-party privacy nonconformities in REG12 at the next management review or within 30 days after escalation, whichever occurs first.

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

10.1.7 [All] The System Owner / Application Owner MUST remove or restrict processor, subprocessor, or third-party access within one business day after an approved suspension, termination, or access-removal decision and MUST record completion evidence in REG08 or REG12.

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 after a material change to processor governance, subprocessor governance, third-party privacy risk, or certification requirements.

11.1.2 [All] The Vendor / Procurement Owner MUST review REG08 relationship field completeness and review-frequency rules annually and within 30 days after a material third-party privacy change.

11.1.3 [Conditional] 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 REG01, REG03, and REG04 within 15 business days after approved policy changes that affect PIMS scope, 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 after publication.

11.1.7 [All] The Vendor / Procurement Owner MUST trigger an out-of-cycle review in REG12 within 10 business days after a major supplier incident, unauthorized subprocessor use, significant contract change, failed exit, customer assurance finding, or audit finding involving processor or subprocessor governance.

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 PII06 - PII Principal Rights 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 PII13 - International PII Transfer Policy

12.11 PII14 - PII Security and Access Control Policy

12.12 PII15 - PII Incident and Breach Management Policy

12.13 PII17 - PIMS Documented Information and Evidence Management Policy

12.14 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 processor, subprocessor, joint controller, and other third-party privacy relationships. Addressed by clauses [4.1.3; 4.1.4; 5.1.2; 7.1.7].

13.2.2 **Clause 6.1.2; Clause 8.2** - Mapped to privacy risk assessment and DPIA screening triggers for processor due diligence, high-risk relationships, and material third-party privacy changes. Addressed by clauses [4.2.1; 4.2.3; 4.2.4; 4.2.6; 6.1.2].

13.2.3 **Clause 7.5; Clause 8.1** - Mapped to documented information and operational control for REG08 relationship records, due diligence, contracts, instructions, subprocessor approvals, monitoring, and exit evidence. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.1.6; 4.2.5; 4.3.7; 7.1.2; 7.1.6].

13.2.4 **Clause 9.1; Clause 10.2** - Mapped to monitoring, measurement, nonconformity, corrective action, escalation, and effectiveness verification for processor and subprocessor governance. Addressed by clauses [4.2.6; 4.5.1; 4.5.7; 6.1.3; 8.1.1; 8.1.8; 10.1.4; 10.1.6].

13.2.5 **Annex A.1.2.7** - Mapped to written contracts with processors, processor contract-control fields, subprocessor-change approval, and contract approval blocking. Addressed by clauses [4.3.1; 4.3.2; 4.3.6; 4.4.6; 10.1.1].

13.2.6 **Annex A.1.2.9** - Mapped to controller-side records for processors, processing relationship linkage, PII categories, processing locations, and assurance evidence. Addressed by clauses [4.1.2; 4.1.6; 4.2.5; 4.5.5; 7.1.7].

13.2.7 **Annex A.2.2.2; Annex A.2.2.3** - Mapped to processor customer agreements, documented customer instructions, and purpose limitation against customer instructions. Addressed by clauses [4.3.3; 4.3.4; 4.3.6; 4.3.7; 7.1.8].

13.2.8 **Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7** - Mapped to infringing-instruction escalation, customer compliance support, and processor records for customer PII processing. Addressed by clauses [4.3.5; 4.3.6; 4.3.7; 4.5.2; 7.1.8].

13.2.9 **Annex A.2.3.2** - Mapped to processor assistance for PII principal rights and related customer-support obligations coordinated through REG08 and REG06. Addressed by clauses [4.3.6; 4.5.2; 5.1.2].

13.2.10 **Annex A.2.4.3** - Mapped to return, transfer, disposal, deletion, transition, and exit evidence for processor and subprocessor relationships. Addressed by clauses [4.3.6; 4.5.6; 8.1.7; 10.1.7].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapped to third-party disclosure records, legally binding disclosure request handling, customer-authorized disclosure handling, and disclosure evidence in REG08. Addressed by clauses [4.5.3; 4.5.5; 7.1.6].

13.2.12 **Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9** - Mapped to subprocessor disclosure, customer authorization, engagement according to contract, and intended subprocessor-change notice and objection handling. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.6].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapped to accountability evidence for processor classification, due diligence, approval, monitoring, exception handling, corrective action, and audit evidence. Addressed by clauses [4.1.3; 4.2.5; 4.5.1; 4.5.7; 6.1.6; 8.1.8; 10.1.4].

13.3.2 **Article 24** - Mapped to controller governance measures for selecting, contracting, monitoring, reviewing, and correcting processors and third-party privacy relationships. Addressed by clauses [4.1.5; 4.2.1; 4.2.3; 4.3.1; 6.1.2; 6.1.7; 11.1.1].

13.3.3 **Article 26** - Mapped to classifying joint controller relationships and routing joint controller responsibility allocation to the appropriate PIMS records and related policies. Addressed by clauses [4.1.3; 4.1.4; 7.1.7].

13.3.4 **Article 28** - Mapped to processor and subprocessor governance, written agreements, documented instructions, subprocessor authorization, customer assistance, audit or assurance, return or deletion, and flow-down contract controls. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.2; 4.4.3; 4.4.4; 4.5.2; 4.5.4; 4.5.6].

13.3.5 **Article 30** - Mapped to processing relationship records, processor records, subprocessor records, processing role classification, PII categories, processing locations, and linkage to REG02 and REG08. Addressed by clauses [4.1.3; 4.1.6; 4.3.3; 4.3.7; 4.5.5; 7.1.7].

13.3.6 **Article 32** - Mapped to security assurance review, security requirements in contracts, subprocessor security evidence, and linkage to PII security and access-control evidence. Addressed by clauses [4.2.2; 4.3.2; 4.3.6; 4.4.4; 4.4.5; 7.1.4; 7.1.5].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.10; Clause 5.11; Clause 5.12** - Mapped to accountability, information security, and privacy compliance for processor due diligence, security assurance, monitoring, audit evidence, corrective action, and compliance review. Addressed by clauses [4.2.1; 4.2.2; 4.2.6; 4.5.7; 6.1.3; 6.1.6; 8.1.8; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Mapped to evaluating PII processors, written processor contracts, subprocessor approval, monitoring and review of supplier services, and managing changes to supplier services. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.4.2; 4.4.4; 4.5.1; 4.5.6; 6.1.5].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23 - Mapped to supplier security risk management, supplier agreement requirements, ICT supply chain controls, supplier service monitoring and change management, and cloud service acquisition, use, management, and exit linkage. Addressed by clauses [4.1.5; 4.2.1; 4.2.2; 4.3.6; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.4; 7.1.5].

13.7 ISO/IEC 27018:2020

13.7.1 **Annex A.2.1; Annex A.3.1** - Mapped to cloud processor cooperation for PII principal rights and cloud processor processing limited to customer purposes and instructions. Addressed by clauses [4.3.3; 4.3.4; 4.5.2; 7.1.8].

13.7.2 **Annex A.6.1; Annex A.6.2; Annex A.8.1** - Mapped to cloud processor disclosure notification, disclosure records, and subcontractor transparency before use. Addressed by clauses [4.4.1; 4.4.3; 4.5.3; 4.5.5].

13.7.3 **Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1** - Mapped to cloud processor breach-interface contract terms, return or disposal evidence, contract measures, sub-contractor flow-down measures, and geographical location records. Addressed by clauses [4.3.6; 4.4.4; 4.5.4; 4.5.5; 4.5.6; 8.1.7].

13.8 ISO/IEC 27036-2:2022

13.8.1 **Clause 6.1.1; Clause 6.1.2** - Mapped to acquisition and supply relationship strategy for processor and subprocessor privacy governance from both acquirer and supplier perspectives. Addressed by clauses [4.1.1; 4.2.1; 4.2.6; 6.1.1; 6.1.2].

13.8.2 **Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5** - Mapped to supplier relationship planning, supplier selection, agreement, relationship management, monitoring, change management, and termination controls for processor and subprocessor relationships. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.3.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 10.1.7].