					Insert Registered Legal Entity Name Here							
Document number: PII23					Document Title: **Cloud PII Processor 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; Clause 6.1.3	Processor	Supporting	PIMS role and control applicability
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Documented cloud processor evidence and operational control
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitoring, nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Customer agreements, instructions, support and records
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Customer assistance for PII principal obligations
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Temporary files, return, transfer, disposal and transmission controls
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Transfer basis and locations
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	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 notice
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Access, records, backup and logging evidence
GDPR	Article 28	Processor	Primary	Processor, subprocessor, assistance, audit, deletion and return
GDPR	Article 30	Processor	Supporting	Processor records

GDPR	Article 32; Article 33	Processor	Supporting	Security and breach notification to controller
GDPR	Article 44	Conditional	Referenced	International transfer routing
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Purpose, minimization, use, retention and disclosure limitation
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Accountability, information security and compliance
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Processor evaluation, monitoring, change and retention controls
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Control applicability, operational control and supplier/cloud controls
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Supplier, cloud, deletion, logging and monitoring controls
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Cloud processor customer assistance and purpose limitation
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	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	Processor	Primary	Cloud breach interface, exit, contract measures, subcontracts and location records
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Supply relationship strategy and governance

ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Supplier relationship planning, agreement, management, monitoring and termination
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Deletion framework and documentation
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Deletion implementation and exceptions

1. Scope

1.1 This policy defines mandatory privacy requirements for cloud services where the organization acts as a PII processor or subprocessor, including SaaS, PaaS, IaaS, hosted application, managed cloud, cloud support, cloud storage, cloud analytics, and cloud infrastructure services that process PII on behalf of customers.

1.2 This policy applies to cloud processing performed under customer agreements, documented customer instructions, upstream processor instructions, subprocessor arrangements, cloud-region configuration, cloud support access, service administration, backup, replication, logging, monitoring, deletion, return, breach support, audit support and customer assistance obligations.

1.3 This policy covers:

1.3.1 cloud PII processing scope and instruction records;

1.3.2 customer agreement and shared-responsibility evidence;

1.3.3 tenant isolation, cloud access, administrative access and logging evidence;

1.3.4 subprocessor and cloud supply-chain governance;

1.3.5 location, remote access and international transfer routing;

1.3.6 return, transfer, deletion, disposal and exit evidence;

1.3.7 customer assistance for PII principal rights, DPIAs, audits and breach response;

1.3.8 monitoring, exception, enforcement and improvement evidence.

1.4 This policy does not create a separate customer contract register, cloud service register, tenant isolation register, access register, log register, deletion register, support request register, audit evidence register, breach register, subprocessor register or cloud governance committee.

1.5 This policy does not replace:

1.5.1 PII03 for processing inventory and lawful-basis ownership;

1.5.2 PII06 for full PII principal rights workflow;

1.5.3 PII07 for privacy risk and DPIA methodology;

1.5.4 PII08 for privacy by design and default gates;

1.5.5 PII09 for general collection, use, disclosure and sharing controls;

1.5.6 PII10 for retention, deletion and disposal methodology;

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

1.5.8 PII13 for international transfer mechanism assessment;

1.5.9 PII14 for full PII security and access control architecture;

1.5.10 PII15 for incident and breach management workflow;

1.5.11 PII17 for documented information control;

1.5.12 PII18 for PIMS monitoring, audit and improvement governance.

2. Purpose

2.1 The purpose of this policy is to ensure that cloud PII processor and subprocessor services are operated under documented customer instructions, clear processing scope, controlled subprocessor arrangements, appropriate cloud security responsibilities, documented location and transfer routing, customer assistance obligations, breach support, deletion/return capability, and audit-ready evidence.

2.2 This policy supports ISO/IEC 27701:2025 PIMS certification readiness for cloud processors and cloud subprocessors while remaining integrated with the existing PIMS policy set and canonical evidence objects.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 Define cloud PII processing scope before customer onboarding or material change.

3.1.2 Ensure customer instructions are recorded, reviewed and followed.

3.1.3 Maintain cloud processor and subprocessor evidence in canonical PIMS registers.

3.1.4 Define shared-responsibility, tenant-isolation, access, logging and location evidence without duplicating the PII security policy.

3.1.5 Control subprocessor onboarding, change, flow-down and monitoring evidence.

3.1.6 Support customers with PII principal rights, DPIAs, audit requests and breach response.

3.1.7 Ensure return, deletion, transfer and disposal evidence is retained at exit.

3.1.8 Monitor cloud processor controls and drive corrective action using REG12.

4. Policy Statements

4.1 Cloud Processing Scope and Customer Instructions

4.1.1 [Processor] The Privacy Lead / PIMS Manager MUST record each cloud PII processing service, customer processing role, customer instruction source, PII categories, PII principal categories, service purpose, processing location, subprocessor dependency, deletion dependency and transfer flag in REG02 and REG08 before customer onboarding or material service change.

4.1.2 [Processor] The Process Owner / Business Owner MUST record the documented customer instructions for cloud PII processing in REG08 before processing begins.

4.1.3 [Subprocessor] The Process Owner / Business Owner MUST record upstream processor or customer-approved instructions in REG08 before processing PII as a cloud subprocessor.

4.1.4 [Processor] The Privacy Lead / PIMS Manager MUST record cloud processor control applicability in REG03 before a new cloud PII processing service is released or materially changed.

4.1.5 [Processor] The Data Protection Officer / Privacy Advisor MUST review any customer instruction that appears inconsistent with documented customer obligations, PIMS requirements or approved service scope in REG12 before the organization acts on the instruction.

4.1.6 [Processor] The Process Owner / Business Owner MUST record any proposed processing of customer PII outside documented customer instructions in REG12 and obtain Privacy Lead / PIMS Manager approval before processing occurs.

4.2 Cloud Configuration, Tenant Isolation, Access and Logging

4.2.1 [Processor] The Information Security Lead MUST record the cloud shared-responsibility boundary for PII access, administration, logging, backup, encryption, vulnerability management and deletion in REG08 before customer onboarding or material service change.

4.2.2 [Processor] The System Owner / Application Owner MUST validate tenant isolation or customer segregation controls in REG12 before production use and after material architecture change.

4.2.3 [Processor] The System Owner / Application Owner MUST grant cloud administrative access to customer PII only after approved business need, access scope, access duration and review frequency are recorded in REG12.

4.2.4 [Processor] The Information Security Lead MUST review privileged cloud access, support access, customer PII access and logging coverage in REG12 at least quarterly.

4.2.5 [Processor] The System Owner / Application Owner MUST validate separation of production, staging, test and support environments for customer PII in REG12 before release and after material environment change.

4.2.6 [Processor] The System Owner / Application Owner MUST record backup, replication, log storage and support-access locations for cloud customer PII in REG02, REG08 or REG09 before enabling or changing those locations.

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

9. Exceptions

9.1 [Processor] The Process Owner / Business Owner MUST request a cloud processor exception in REG12 before onboarding, release, renewal or continued use when required customer instruction, subprocessor, location, access, logging, deletion or incident-interface evidence is incomplete.

9.2 [Processor] The Data Protection Officer / Privacy Advisor MUST review privacy-significant cloud processor exception requests in REG12 before approval when the exception affects customer instructions, PII principal assistance, transfers, subprocessors, deletion, breach support or high-impact PII.

9.3 [Processor] Top Management MUST approve high-risk or material cloud processor exceptions in REG12 before the exception becomes effective.

9.4 [Processor] The Privacy Lead / PIMS Manager MUST assign an expiry date, remediation owner, review date and residual-risk note in REG12 for every approved cloud processor exception before approval.

10. Enforcement

10.1 [Processor] The Privacy Lead / PIMS Manager MUST block customer onboarding, service release, renewal or continued processing when required REG02, REG03, REG08, REG09, REG10 or REG12 evidence is missing before processing begins or continues.

10.2 [Processor] The System Owner / Application Owner MUST disable unapproved cloud access, unapproved region use, unapproved replication, unapproved support access or unapproved subprocessor data flow within one business day after an enforcement decision and record completion in REG08 or REG12.

10.3 [Processor] The Vendor / Procurement Owner MUST suspend new PII processing by an unapproved or nonconforming cloud subprocessor until REG08 corrective action evidence is complete.

10.4 [Processor] The Incident Response Coordinator MUST escalate missed customer incident notification deadlines in REG10 and REG12 within one business day after identification.

10.5 [Processor] The Internal Audit / Compliance Reviewer MUST verify corrective action effectiveness for major or repeated cloud processor nonconformities in REG12 within 60 days after corrective action closure.

11. Review and Maintenance

11.1 [Processor] The Privacy Lead / PIMS Manager MUST review this policy in REG12 annually and within 30 days after a material change to cloud processor obligations, cloud architecture, subprocessor governance, customer assistance, deletion capability or certification requirements.

11.2 [Processor] The Vendor / Procurement Owner MUST review cloud subprocessor and cloud service dependency records in REG08 at least annually and before renewal.

11.3 [Processor] The System Owner / Application Owner MUST review tenant isolation, privileged access, logging, backup, replication and deletion evidence in REG12 at least annually and after material architecture change.

11.4 [Processor] The Privacy Lead / PIMS Manager MUST review REG09 cloud location and transfer routing records at least annually and within 15 business days after a material location, support access, backup or subprocessor change.

11.5 [Processor] The Privacy Lead / PIMS Manager MUST update REG03 within 15 business days after approved policy changes that affect cloud processor control applicability.

11.6 [All] Top Management MUST approve material revisions to this policy in REG12 before 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 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 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.11 PII13 - International PII Transfer Policy

12.12 PII14 - PII Security and Access Control Policy

12.13 PII15 - PII Incident and Breach Management Policy

12.14 PII17 - PIMS Documented Information and Evidence Management Policy

12.15 PII18 - PIMS Monitoring, Audit and Improvement Policy

12.16 PII20 - Children's Privacy Policy

12.17 PII21 - AI and Automated Decision-Making Privacy Policy

12.18 PII22 - Marketing Privacy and Cookies Policy

12.19 PII24 - CCTV and Physical Monitoring Privacy 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 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].