					Insert Registered Legal Entity Name Here							
Document number: PII21					Document Title: **AI and Automated Decision-Making Privacy 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 AI, profiling and automated decision-making processing evidence
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, nonconformity and corrective action for AI privacy controls
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Purpose, lawful basis, privacy impact assessment and controller records
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Processor contracts and joint-controller responsibilities for AI-related PII processing
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Obligations to PII principals and transparency for AI-related processing
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Objection, access, correction, erasure, request handling and automated decision-making obligations
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 for AI inputs, outputs and derived data
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	International transfer, disclosure and disclosure request routing for AI-related PII

ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Processor agreement, documented instructions, customer obligation support and records
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Processor support for principal obligations, transfer routing and disclosure handling
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protection of records and logging related to AI-related PII processing
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profiling, fairness, transparency, purpose limitation, minimization, accuracy and accountability
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Lawfulness, special-category data and criminal conviction or offence data safeguards
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Transparent information, access and meaningful information about automated decision-making
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Rectification, erasure, restriction, objection and automated decision-making rights
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Controller responsibility, design/default, joint controllers, processors, records, security,

				DPIA and DPO tasks
GDPR	Article 44	Conditional	Referenced	International transfer routing for AI-related PII processing
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Purpose, collection, minimization, use, retention, disclosure, accuracy and quality principles
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparency, individual participation, accountability, information security and privacy compliance
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA benefit, threshold determination and preparation for AI-related privacy risk assessment
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Purpose, collection, minimization, use, retention, disclosure, accuracy and principal participation controls

1. Scope

1.1 This policy defines mandatory privacy requirements for artificial intelligence, profiling, scoring, recommendation, decision-support, and automated decision-making processing activities that use, infer, generate, disclose, or otherwise process PII within the PIMS scope.

1.2 This policy applies to:

1.2.1 AI-enabled systems, applications, models, services, workflows, decision engines, scoring tools, recommender systems, analytics models and automated decision-making processes that process PII;

1.2.2 profiling, segmentation, classification, prediction, inference, personalization, ranking, eligibility, fraud detection, risk scoring, access decisions, employment-related assessment, child-related profiling, marketing personalization and similar processing where PII is involved;

1.2.3 AI-related PII used for training, testing, validation, tuning, monitoring, production inference, output review, performance measurement, incident investigation or model retirement;

1.2.4 controller, joint controller, processor and subprocessor contexts;

1.2.5 AI-related vendors, processors, subprocessors, data-sharing recipients and international transfer routes that process PII.

1.3 This policy does not create a full AI governance framework, AI management system, AI inventory, model inventory, model risk register, fairness register, algorithm register, AI incident register, AI committee, model owner role, AI system owner role, legal-advice workflow or separate AI approval form.

1.4 This policy does not replace:

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

1.4.2 PII04 for privacy notice governance;

1.4.3 PII05 for consent and preference management;

1.4.4 PII06 for PII principal rights workflow;

1.4.5 PII07 for privacy risk assessment and DPIA methodology;

1.4.6 PII08 for privacy by design and default gates;

1.4.7 PII09 for collection, use, disclosure and sharing controls;

1.4.8 PII10 for retention, deletion and disposal execution;

1.4.9 PII11 for accuracy and quality controls;

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

1.4.11 PII13 for international transfer controls;

1.4.12 PII14 for security and access control;

1.4.13 PII15 for incident and breach handling;

1.4.14 PII18 for monitoring, audit and improvement;

1.4.15 PII19 for employee privacy;

1.4.16 PII20 for children's privacy;

1.4.17 PII22 for marketing privacy and cookies.

2. Purpose

2.1 The purpose of this policy is to ensure that AI, profiling and automated decision-making activities involving PII are identified, documented, risk-assessed, transparent, contestable, monitored, and controlled through the PIMS without creating duplicate AI-specific governance artifacts.

2.2 This policy ensures that privacy obligations for AI-related PII processing are evidenced through REG02, REG04, REG06, REG07, REG08, REG09, REG10 and REG12.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 identify AI, profiling and automated decision-making processing involving PII in REG02;

3.1.2 document AI-related purposes, lawful basis, PII categories, data sources, inferred data, outputs, recipients and decision effects in REG02;

3.1.3 trigger privacy risk screening and DPIA routing through REG04;

3.1.4 ensure AI-related privacy notices and meaningful information are recorded in REG07;

3.1.5 route rights, objection, human review and contestability requests through REG06;

3.1.6 control AI-related processors, subprocessors, vendors and data-sharing arrangements through REG08;

3.1.7 route AI-related international transfers through REG09;

3.1.8 escalate suspected AI-related PII incidents, misuse, unauthorized disclosure and adverse privacy outcomes through REG10 and REG12;

3.1.9 record monitoring, exceptions, nonconformities, corrective actions and improvements in REG12.

4. Policy Statements

4.1 AI, profiling and automated decision-making identification

4.1.1 [Controller] When a new or materially changed system, application, model, workflow, service or business process is proposed, the Process Owner / Business Owner must determine whether it uses AI, profiling, scoring, recommendation, decision-support or automated decision-making involving PII and record the determination in REG02.

4.1.2 [Controller] Before AI-related PII processing begins, the Process Owner / Business Owner must document the processing purpose, PII categories, PII principal categories, data sources, inferred or derived data categories, output categories, recipient categories, lawful basis and retention linkage in REG02.

4.1.3 [Controller] Before profiling, scoring, recommendation, decision-support or automated decision-making is used in production, the Process Owner / Business Owner must document the decision context, expected effect on PII principals, human involvement and rights route in REG02 and REG04.

4.1.4 [Joint Controller] Before AI-related PII processing is performed with a joint controller, the Privacy Lead / PIMS Manager must document responsibility for purpose definition, notice, rights handling, DPIA support, processor governance and incident escalation in REG08.

4.1.5 [Processor] Before processing PII through an AI-related service for a customer, the Process Owner / Business Owner must confirm that customer instructions, permitted purposes, prohibited uses, output handling and assistance obligations are documented in REG08.

4.1.6 [Both] Before AI-related PII processing is activated, the Privacy Lead / PIMS Manager must confirm that the processing is linked to the applicable canonical evidence objects and that no separate AI-specific register is created outside REG02, REG04, REG06, REG07, REG08, REG09, REG10 or REG12.

4.2 Privacy risk assessment and DPIA routing

4.2.1 [Controller] Before launching or materially changing AI-related PII processing, the Privacy Lead / PIMS Manager must complete privacy risk screening and record the DPIA decision in REG04.

4.2.2 [Conditional] When AI-related processing involves profiling, automated decisions, large-scale evaluation, special-category data, criminal offence data, vulnerable PII principals,

employee assessment, children, behavioral monitoring, location data, biometric data, high-impact scoring or significant effects, the Data Protection Officer / Privacy Advisor must review the privacy risk and record advice in REG04.

4.2.3 [Controller] Before production go-live for AI-related PII processing, the Process Owner / Business Owner must document risk treatment actions, residual risk status and go-live readiness evidence in REG04 or REG12.

4.2.4 [Controller] Before PII is reused for AI training, testing, validation, tuning, monitoring or model improvement for a new or materially changed purpose, the Process Owner / Business Owner must complete privacy review and record the decision in REG02 and REG04.

4.2.5 [Conditional] When residual privacy risk remains high after planned treatment, Top Management must approve, reject or require further treatment before production use and record the decision in REG04 and 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 [All] Before deviating from an AI-related privacy requirement in this policy, the requesting Process Owner / Business Owner must submit an exception rationale and compensating control evidence in REG12.

9.2 [Conditional] When an exception affects profiling, automated decision-making, human review, contestability, transparency, DPIA outcome, high-impact scoring, child-related processing, employee-related processing, processor restrictions or international transfers, the Data Protection Officer / Privacy Advisor must review the exception and record advice in REG04 or REG12.

9.3 [Conditional] When an exception creates or preserves high residual privacy risk, Top Management must approve or reject the exception and record the decision in REG04 and REG12.

9.4 [All] Before an approved AI-related privacy exception expires, the Privacy Lead / PIMS Manager must review closure, renewal or corrective action status and record the outcome in REG12.

10. Enforcement

10.1 [All] When noncompliance with this policy is identified, the Privacy Lead / PIMS Manager must record the nonconformity and corrective action in REG12.

10.2 [Both] When unauthorized AI-related PII processing, disclosure, access, model misuse, rights failure or adverse privacy outcome is suspected, the Incident Response Coordinator must initiate incident escalation and record evidence in REG10 and REG12.

10.3 [Both] When a processor, subprocessor, supplier or data-sharing recipient fails to meet AI-related privacy obligations, the Vendor / Procurement Owner must record remediation, escalation or termination action in REG08 and REG12.

10.4 [All] When repeated or systemic AI-related privacy nonconformities occur, Top Management must review the issue and record the management action in REG12.

11. Review and Maintenance

11.1 [All] At least annually, the Privacy Lead / PIMS Manager must review this policy for continued suitability and record the review outcome in REG12.

11.2 [Conditional] When laws, services, models, data sources, profiling practices, automated decision-making logic, vendor arrangements, transfer routes or privacy risks materially change, the Privacy Lead / PIMS Manager must review affected AI-related privacy controls and record the outcome in REG02, REG04 or REG12.

11.3 [Controller] At least annually and after material AI-related user journey changes, the Process Owner / Business Owner must review transparency, meaningful information, human review and rights route evidence and record the review in REG06 and REG07.

11.4 [All] After AI-related privacy corrective actions are closed, the Internal Audit / Compliance Reviewer must verify effectiveness and record verification evidence in REG12.

12. Related Policies

12.1 PII01 - Privacy Information Management System Policy

12.2 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.3 PII03 - PII Processing Inventory and Lawful Basis Policy

12.4 PII04 - Privacy Notice and Transparency Policy

12.5 PII05 - Consent and Preference Management 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 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

12.18 PII19 - Employee Privacy Policy

12.19 PII20 - Children's Privacy Policy

12.20 PII22 - Marketing Privacy and Cookies Policy

13. Reference Standards and Frameworks

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].