					Insert Registered Legal Entity Name Here							
Document number: PII07					Document Title: **Privacy Risk Assessment and DPIA 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 6.1.1	Both	Primary	PIMS risks and opportunities
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Privacy risk assessment
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Privacy risk treatment and SoA linkage
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Planned PIMS changes and risk reassessment
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Privacy risk and DPIA documented information
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operational planning and control
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operational privacy risk assessment
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operational privacy risk treatment
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Privacy risk monitoring and measurement
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Management review of privacy risk
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Risk-related nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Privacy impact assessment
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Processing records supporting risk assessment
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Processor customer agreement and DPIA assistance
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Processor information supporting

				customer compliance
GDPR	Article 5(2)	Controller	Supporting	Accountability evidence
GDPR	Article 24	Controller	Supporting	Controller responsibility and measures
GDPR	Article 25	Controller	Supporting	Data protection by design and default
GDPR	Article 28	Both	Supporting	Processor assistance and instructions
GDPR	Article 30	Both	Supporting	Processing records supporting DPIA
GDPR	Article 32	Both	Supporting	Security risk and safeguards
GDPR	Article 35	Controller	Primary	Data protection impact assessment
GDPR	Article 36	Controller	Primary	Prior consultation
GDPR	Article 39	Conditional	Supporting	DPO advice and monitoring where applicable
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Privacy controls, information security and privacy compliance
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA scope, benefits, trigger and preparation
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII protection programme and requirement identification
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Organizational privacy risk management integration

1. Scope

1.1 This policy defines the requirements for privacy risk assessment, DPIA screening, full DPIA execution, risk treatment, residual risk acceptance, consultation, review, and evidence management for PII processing within the PIMS scope.

1.2 This policy applies to the following:

1.2.1 new and materially changed PII processing activities;

1.2.2 controller, joint controller, processor, and subprocessor processing contexts;

1.2.3 systems, applications, services, business processes, suppliers, processors, subprocessors, international transfers, and data-sharing arrangements that affect PII processing;

1.2.4 privacy risk and DPIA evidence maintained in REG04 and supporting evidence maintained in REG02, REG03, REG08, REG09, REG10, REG11, and REG12.

1.3 This policy does not replace processing inventory controls, privacy notice controls, consent controls, PII principal rights controls, privacy-by-design controls, supplier controls, international transfer controls, PII security controls, incident controls, documented information controls, or monitoring/audit/improvement controls. Those requirements are defined in the related policies listed in Section 12.

1.4 For this policy, privacy risk assessment means the documented identification, analysis, evaluation, treatment, review, and monitoring of potential adverse privacy impacts arising from PII processing.

1.5 For this policy, DPIA means a documented assessment used for controller processing that is likely to result in high risk to PII principals and that evaluates processing necessity, proportionality, risks, safeguards, residual risk, consultation needs, and approval conditions.

1.6 For this policy, high residual privacy risk means a privacy risk that remains above the approved acceptance threshold after proposed or implemented risk treatment.

1.7 For this policy, a material change means any change affecting PIMS scope, processing purpose, lawful basis, PII categories, PII principal categories, processing scale, processing technology, monitoring or profiling, automated decision-making, vulnerable PII principals, recipients, processors, subprocessors, international transfers, retention, security controls, risk profile, customer instructions, or certification scope.

2. Purpose

2.1 The purpose of this policy is to ensure that privacy risks and DPIA obligations are identified, assessed, treated, approved, reviewed, and evidenced before PII processing creates unacceptable risk to PII principals or to the PIMS.

2.2 This policy enables the organization to demonstrate risk-based privacy governance, controller DPIA accountability, processor DPIA assistance, documented risk treatment, residual risk approval, prior consultation decision-making, and continual improvement of privacy controls.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define mandatory privacy risk screening triggers;

3.1.2 define when a full DPIA is required;

3.1.3 ensure controller DPIA decisions are documented and reviewable;

3.1.4 ensure processor and subprocessor DPIA assistance is documented where required by customer instruction or agreement;

3.1.5 ensure privacy risks are assessed before new or materially changed PII processing proceeds;

3.1.6 ensure privacy risk treatments are assigned, implemented, and verified;

3.1.7 ensure high residual privacy risks are escalated and approved before processing begins or continues;

3.1.8 ensure prior consultation decisions are documented where high residual risk remains;

3.1.9 ensure privacy risk and DPIA evidence is maintained in REG04 and linked to related evidence objects;

3.1.10 avoid creating separate DPIA, risk, or consultation registers outside REG04.

4. Policy Statements

4.1 Privacy risk screening

4.1.1 [Both] The Process Owner / Business Owner MUST initiate privacy risk screening in REG04 before new or materially changed PII processing recorded in REG02 begins.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUST maintain privacy risk screening criteria in REG04 before initial PIMS operation and annually thereafter.

4.1.3 [Controller] The Process Owner / Business Owner MUST complete DPIA screening in REG04 before controller processing that meets privacy risk screening criteria begins.

4.1.4 [Processor] The Vendor / Procurement Owner MUST record customer DPIA assistance requirements in REG08 before processor processing begins where the customer agreement or documented instruction requires DPIA support.

4.1.5 [Both] The System Owner / Application Owner MUST provide system design, access, security, logging, and data-flow evidence in REG04 before privacy risk assessment approval for new or materially changed systems processing PII.

4.1.6 [Both] The Privacy Lead / PIMS Manager MUST record the screening outcome and full-DPIA decision rationale in REG04 before the processing activity proceeds.

4.2 DPIA triggers and requirement determination

4.2.1 [Controller] The Privacy Lead / PIMS Manager MUST require a full DPIA in REG04 before controller processing likely to result in high risk begins.

4.2.2 [Controller] The Process Owner / Business Owner MUST refer processing involving large scale, systematic monitoring, profiling, automated decisions, special category PII, criminal conviction or offence data, vulnerable PII principals, innovative technology, or materially changed processing to the Privacy Lead / PIMS Manager in REG04 before processing begins.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST record advice in REG04 before approval of a full-DPIA requirement decision for high-risk controller processing.

4.2.4 [Both] The Process Owner / Business Owner MUST re-screen privacy risk in REG04 before using PII for a new purpose, adding a new recipient, introducing a new processor or subprocessor, changing system architecture, or starting a new international transfer.

4.2.5 [Processor] The Privacy Lead / PIMS Manager MUST document whether processor DPIA support is required in REG08 within 10 business days of receiving a customer DPIA assistance request.

4.2.6 [Subprocessor] The Vendor / Procurement Owner MUST document upstream DPIA assistance requirements in REG08 before subprocessing begins where the upstream customer or processor agreement requires such assistance.

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

9. Exceptions

9.1 Privacy risk and DPIA exceptions

9.1.1 [All] The Process Owner / Business Owner MUST request any exception to this policy in REG12 before the deviation occurs.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST assess the privacy, legal, certification, operational, and PII principal impact of each requested exception in REG04 or REG12 within 10 business days of request.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of any exception affecting high-risk processing, full DPIA completion, prior consultation, high residual privacy risk, or customer DPIA assistance.

9.1.4 [All] Top Management MUST approve privacy risk or DPIA exceptions affecting high-risk processing, certification scope, prior consultation, or unresolved high residual privacy risk in REG12 before the exception takes effect.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST set an expiry date not exceeding 90 days in REG12 for each approved privacy risk or DPIA exception before approval.

9.1.6 [All] The Process Owner / Business Owner MUST close or reassess each privacy risk or DPIA exception in REG12 within five business days of expiry.

10. Enforcement

10.1 Privacy risk and DPIA enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record missing, inaccurate, incomplete, overdue, or unapproved REG04 privacy risk or DPIA evidence as a nonconformity in REG12 within five business days of identification.

10.1.2 [Controller] The Process Owner / Business Owner MUST suspend new high-risk controller processing when required REG04 DPIA approval evidence is missing before launch.

10.1.3 [Both] The System Owner / Application Owner MUST block go-live of systems processing PII when required REG04 risk treatment evidence is missing before go-live approval.

10.1.4 [Both] The Vendor / Procurement Owner MUST block supplier, processor, subprocessor, or data-sharing onboarding when required REG04 privacy risk or DPIA assistance evidence is missing before agreement approval.

10.1.5 [All] Top Management MUST review unresolved major privacy risk or DPIA nonconformities in REG12 during management review.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST escalate repeated missed REG04 screening, DPIA review, or risk treatment deadlines to Top Management in REG12 within five business days after the second occurrence in a 12-month period.

10.1.7 [All] The Internal Audit / Compliance Reviewer MUST verify corrective action effectiveness for privacy risk and DPIA nonconformities in REG12 at the next scheduled audit or within 60 days of closure, whichever occurs first.

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 of material change to privacy risk, DPIA, prior consultation, processor assistance, or certification requirements.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST review REG04 screening criteria, DPIA trigger criteria, risk rating criteria, and residual risk acceptance criteria in REG12 annually.

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 update REG03 and REG04 within 15 business days after approved policy changes that alter control applicability, risk criteria, or DPIA 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 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 PII06 - PII Principal Rights Management 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

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 6.1.1** - Mapped to identifying and planning actions for privacy risks and opportunities using screening criteria, risk thresholds, escalation, and management review inputs. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mapped to conducting privacy risk screening, privacy risk assessment, risk rating, reassessment, and DPIA trigger evaluation before new or materially changed processing proceeds. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mapped to privacy risk treatment planning, control applicability updates, treatment implementation, residual risk acceptance, and SoA linkage. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mapped to planned PIMS and processing changes triggering privacy risk reassessment and DPIA review. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapped to controlled documented information for privacy risk screening, DPIA evidence, risk treatment, residual risk acceptance, prior consultation decisions, exceptions, nonconformities, and policy review evidence. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mapped to operating privacy risk and DPIA controls before go-live, onboarding, processing approval, treatment closure, and corrective action linkage. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mapped to operational privacy risk assessment for new, changed, system, supplier, transfer, and incident-driven processing changes. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mapped to operational privacy risk treatment, treatment assignment, treatment implementation, overdue treatment escalation, and effectiveness verification. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mapped to monitoring and measuring screening coverage, DPIA status, open risks, overdue treatment actions, supplier actions, security treatment actions, incident reassessment actions, and audit findings. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mapped to management review of high residual privacy risks, overdue treatment actions, full DPIA status, prior consultation decisions, and major privacy risk exceptions. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapped to privacy risk and DPIA nonconformities, exceptions, corrective action opening, escalation, and effectiveness verification. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mapped to assessing the need for, and implementing where appropriate, privacy impact assessment for new or changed controller processing. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mapped to processing records supporting privacy risk and DPIA assessment inputs, including purpose, categories, systems, recipients, transfers, and suppliers. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapped to processor customer agreements and customer DPIA assistance obligations. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mapped to processor provision of information needed for customer compliance, including DPIA assistance and customer support evidence. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapped to accountability evidence for DPIA screening, full-DPIA decisions, risk treatment, residual risk acceptance, prior consultation decisions, exceptions, audit findings, and corrective actions. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mapped to controller responsibility for appropriate privacy risk measures, high residual risk review, management approval, and policy maintenance. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mapped to privacy-by-design and privacy-by-default evidence used in risk assessment and before go-live approval. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapped to processor and subprocessor DPIA assistance, customer instruction handling, and supplier risk treatment evidence. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mapped to processing records supporting privacy risk assessment and DPIA inputs. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapped to PII security risk inputs, safeguard selection, security risk treatment, and security control status updates. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapped to DPIA screening, full DPIA requirement determination, DPIA content, DPO advice, review, and blocking high-risk processing without required DPIA approval. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mapped to prior consultation decision-making, DPO advice, Top Management approval, and continuation, suspension, redesign, or consultation actions where high residual risk remains. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapped to Data Protection Officer / Privacy Advisor advice and monitoring where applicable for DPIA decisions, high-risk processing, prior consultation, and policy changes. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mapped to privacy control identification, security safeguards, privacy compliance, privacy risk evidence, monitoring, and review. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapped to the PIA process scope, benefits, trigger determination, preparation, assessment inputs, stakeholder evidence, and DPIA report structure maintained in REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Mapped to PII protection programme requirements, PII protection requirement identification, risk-based control selection, and privacy risk treatment linkage. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mapped to organizational privacy risk principles, leadership, integration, risk assessment, risk treatment, monitoring and review, and recording and reporting. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].