					Insert Registered Legal Entity Name Here							
Document number: PII16					Document Title: **Privacy Training, Awareness and Competence 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 7.2; Clause 7.3	Both	Primary	Competence and awareness
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Communication and documented evidence
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operational control, measurement and improvement
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	PII processing awareness, education and training
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Accountability, processor governance, security and DPO tasks
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Competence, awareness and training
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Awareness, education and training guidance
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Information security and privacy compliance

1. Scope

1.1 This policy defines the organization's requirements for privacy training, awareness and competence within the Privacy Information Management System.

1.2 This policy applies to personnel, contractors, temporary personnel, relevant third parties, processors, subprocessors and other interested parties whose work can affect PII processing, PIMS performance, PII principal rights, privacy risk, information security related to PII, processor instructions, privacy incidents, documented information or compliance evidence.

1.3 This policy applies to controller, joint controller, processor and subprocessor contexts.

1.4 This policy covers:

1.4.1 privacy training audience identification;

1.4.2 onboarding training;

1.4.3 annual refresher training;

1.4.4 role-based and event-triggered training;

1.4.5 training completion evidence;

1.4.6 non-completion escalation;

1.4.7 training effectiveness review;

1.4.8 processor, subprocessor and third-party training assurance evidence.

1.5 This policy does not create a separate training matrix, training dashboard, human resources register, competence register, disciplinary register or customer training register. Training assignments, completions, reminders, competence evidence and awareness evidence are recorded in REG11, with exceptions, escalations, nonconformities, corrective actions and review evidence recorded in REG12. Processor, subprocessor and third-party training assurance evidence is recorded in REG08 where relevant.

1.6 This policy does not duplicate:

1.6.1 role-accountability assignment in PII02;

1.6.2 processing inventory and lawful-basis requirements in PII03;

1.6.3 privacy-risk and DPIA methodology in PII07;

1.6.4 privacy-by-design gates in PII08;

1.6.5 processor lifecycle governance in PII12;

1.6.6 PII security and access-control operation in PII14;

1.6.7 PII incident and breach workflow in PII15;

1.6.8 documented information governance in PII17;

1.6.9 monitoring, internal audit and improvement governance in PII18.

2. Purpose

2.1 The purpose of this policy is to ensure that people whose work affects PII processing understand their privacy responsibilities, complete appropriate training on a defined cadence, maintain role-relevant competence and generate auditable evidence of training, awareness and escalation.

2.2 This policy supports consistent PIMS implementation by using REG11 as the primary training and awareness evidence object and REG08, REG10 and REG12 as supporting evidence objects.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define privacy training audiences;

3.1.2 define onboarding training requirements;

3.1.3 define annual refresher training requirements;

3.1.4 define role-based privacy training requirements;

3.1.5 record completion evidence in REG11;

3.1.6 escalate non-completion through REG12;

3.1.7 maintain processor, subprocessor and third-party training assurance evidence in REG08 where relevant;

3.1.8 review training effectiveness without creating excessive metrics or duplicate registers;

3.1.9 ensure training content remains aligned with current PIMS policies and material privacy obligations.

4. Policy Statements

4.1 Training audience and assignment

4.1.1 [All] The Privacy Lead / PIMS Manager MUST define PIMS training audience categories in REG11 before each annual training cycle begins.

4.1.2 [All] The Process Owner / Business Owner MUST identify personnel whose duties involve PII processing in REG11 before onboarding, role assignment or material duty change.

4.1.3 [Conditional] The System Owner / Application Owner MUST identify users requiring PII system, privileged-access or administrative privacy training in REG11 before access is enabled or materially changed.

4.1.4 [Joint Controller] The Privacy Lead / PIMS Manager MUST record joint-controller training responsibility allocation in REG11 or REG08 before joint processing activity begins or materially changes.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST identify enhanced privacy training needs in REG11 before training is assigned to roles handling high-risk processing, special-category PII, PII principal rights, DPIAs, international transfers or breach assessment.

4.1.6 [All] The Privacy Lead / PIMS Manager MUST record the assigned training audience, training type, required completion date and evidence owner in REG11 before each annual training cycle begins.

4.2 Onboarding and annual training cadence

4.2.1 [All] The Privacy Lead / PIMS Manager MUST assign baseline privacy awareness training in REG11 within 10 business days of onboarding for personnel with access to PII or PIMS responsibilities.

4.2.2 [All] The Process Owner / Business Owner MUST ensure assigned personnel complete onboarding privacy training in REG11 before unsupervised access to PII is approved or within 30 days of onboarding, whichever occurs first.

4.2.3 [All] The Privacy Lead / PIMS Manager MUST assign annual privacy refresher training in REG11 at least once every 12 months.

4.2.4 [All] The Process Owner / Business Owner MUST confirm annual refresher completion status for assigned personnel in REG11 by the published annual due date.

4.2.5 [Conditional] The Privacy Lead / PIMS Manager MUST assign targeted refresher training in REG11 within 30 days after a material privacy policy change, material PIMS process change, audit finding, recurring training failure or relevant PII incident lesson.

[... 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 record a privacy training exception request in REG12 before a required completion deadline is extended.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST approve or reject privacy training exception requests in REG12 before the exception becomes active.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST advise on training exceptions in REG12 before approval where the exception affects high-risk processing, special-category PII, rights handling, incident handling, international transfers or certification evidence.

9.1.4 [Conditional] Top Management MUST approve privacy training exceptions in REG12 before activation when the exception affects repeated non-completion, privileged PII access, high-impact PII processing or regulatory-facing evidence.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST define exception owner, expiry date, compensating action and review date in REG12 before approving any privacy training exception.

9.1.6 [All] The Process Owner / Business Owner MUST close or renew approved privacy training exceptions in REG12 before the exception expiry date.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record a training nonconformity in REG12 within five business days when mandatory privacy training evidence is missing, incomplete, overdue or not traceable to REG11.

10.1.2 [All] The Process Owner / Business Owner MUST ensure overdue mandatory privacy training is completed or escalated in REG11 or REG12 within 10 business days after overdue status is recorded.

10.1.3 [Conditional] The System Owner / Application Owner MUST restrict new high-impact PII access in REG12 when required onboarding or role-based privacy training remains incomplete after escalation.

10.1.4 [Processor] The Vendor / Procurement Owner MUST escalate missing processor, subprocessor or external workforce training assurance evidence in REG08 and REG12 within five business days after identification.

10.1.5 [Conditional] The Incident Response Coordinator MUST link training-related enforcement actions to REG10 within one business day when the training failure contributed to a suspected or confirmed PII incident.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verify closure evidence for training corrective actions in REG12 at the next scheduled audit or within 60 days of closure, whichever occurs first.

11. Review and Maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy and training content at least annually and record the review outcome in REG11 or REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST review this policy within 30 days after a material change to PIMS scope, privacy law, processing activities, role model, incident lessons, audit findings or training effectiveness results.

11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST review privacy-significant policy changes 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 REG11 training content and assignment evidence within 30 days after an approved material policy change.

12. Related Policies

12.1 This policy should be read with:

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 PII07 - Privacy Risk Assessment and DPIA Policy;

12.9 PII08 - Privacy by Design and Default Policy;

12.10 PII09 - PII Collection, Use, Disclosure and Sharing Policy;

12.11 PII10 - PII Retention, Deletion and Disposal 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 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].