					Insert Registered Legal Entity Name Here							
Document number: PII19					Document Title: **Employee 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	Employee privacy evidence and operational control
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	HR purposes, lawful-basis linkage, DPIA trigger, joint responsibility and records
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	HR processor contracts, instructions, assistance and records
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Employee obligations, rights and automated-decision routing
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Collection, processing, minimization and retention linkage
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Disclosure records and legally binding disclosure handling
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	HR record protection and logging evidence
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Employee privacy principles and accountability
GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Lawfulness, special-category and background-screening data

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Employee transparency and notices
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Employee rights and automated-decision routing
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governance, joint controllers, processors, records, security, DPIA and advice
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Purpose, collection, minimization, use, retention and disclosure
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparency, participation, accountability, security and compliance
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	PII purpose, collection, minimization, retention and principal participation
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	PII-protective workforce lifecycle controls
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	HR processor evaluation, monitoring and change control
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	HR privacy risk and DPIA trigger linkage
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	PII protection and workforce information-security lifecycle
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Logging and monitoring activities

1. Scope

1.1 This policy defines employee privacy requirements for the collection, use, disclosure, retention linkage, notice, rights handling, monitoring, processor support and evidence management of employee PII within the Privacy Information Management System.

1.2 For this policy, “employee PII” includes PII relating to employees, job applicants, former employees, contractors, temporary personnel, interns, secondees and other workforce participants where the organization processes their PII for workforce, recruitment, employment, engagement, compensation, benefits, security, compliance, workplace administration or related business purposes.

1.3 This policy applies to controller and joint-controller contexts where the organization determines the purposes and means of employee PII processing.

1.4 This policy also applies to processor and subprocessor contexts where the organization processes employee PII on behalf of a customer, upstream processor or other controller under documented instructions.

1.5 This policy covers:

1.5.1 employee data collection;

1.5.2 HR processing purposes;

1.5.3 employee privacy notices;

1.5.4 employee rights handling;

1.5.5 retention linkage;

1.5.6 employee monitoring;

1.5.7 internal disclosure;

1.5.8 HR processor, payroll, HRIS, benefits, background screening and outsourced HR service controls where applicable;

1.5.9 employee PII incidents, nonconformities, corrective actions and improvement evidence.

1.6 This policy does not create a separate HR privacy register, employee privacy register, HR processing register, employee monitoring register, background-screening register, HR vendor register, employee rights register or employee incident register. Employee processing evidence is recorded in REG02, REG04, REG06, REG07, REG08, REG10 and REG12.

1.7 This policy does not provide employment-law advice, labour-relations advice, works council legal commentary, disciplinary procedure content, payroll operating procedure content or jurisdiction-specific employment-document templates.

1.8 This policy does not duplicate:

1.8.1 PIMS governance in PII01;

1.8.2 role accountability in PII02;

1.8.3 processing inventory and lawful-basis ownership in PII03;

1.8.4 privacy notice content governance in PII04;

1.8.5 consent and preference operation in PII05;

1.8.6 PII principal rights workflow in PII06;

1.8.7 privacy risk and DPIA methodology in PII07;

1.8.8 privacy-by-design gates in PII08;

1.8.9 collection, use, disclosure and sharing baseline rules in PII09;

1.8.10 retention, deletion and disposal execution in PII10;

1.8.11 accuracy and quality governance in PII11;

1.8.12 processor, subprocessor and third-party lifecycle governance in PII12;

1.8.13 international transfer mechanism controls in PII13;

1.8.14 security and access-control implementation in PII14;

1.8.15 incident and breach handling in PII15;

1.8.16 training and awareness management in PII16;

1.8.17 documented information control in PII17;

1.8.18 PIMS monitoring, audit and improvement governance in PII18;

1.8.19 AI and automated decision-making controls in PII21, where that optional policy is included.

2. Purpose

2.1 The purpose of this policy is to ensure that employee PII is processed only for documented, approved, transparent, proportionate and accountable workforce purposes, and that employee privacy evidence is maintained in the canonical PIMS registers without creating a separate HR privacy evidence layer.

2.2 This policy supports consistent handling of employee processing by linking employee processing activities to REG02, employee privacy notices to REG07, employee rights requests to REG06, HR privacy risk and DPIA triggers to REG04, HR processors and payroll or HRIS vendors to REG08, employee PII incidents to REG10, and exceptions, nonconformities, corrective actions and monitoring evidence to REG12.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 maintain employee processing inventory evidence in REG02;

3.1.2 document employee collection sources, PII categories, purposes, systems, recipients and retention linkage;

3.1.3 maintain employee privacy notice evidence in REG07;

3.1.4 route employee privacy risk and DPIA triggers through REG04;

3.1.5 route employee rights requests through REG06;

3.1.6 maintain HR processor, payroll, HRIS, benefits, background screening and outsourced HR service evidence in REG08;

3.1.7 ensure employee monitoring is documented, proportionate, reviewed and escalated through REG04 and REG12 where applicable;

3.1.8 route suspected employee PII incidents through REG10;

3.1.9 record employee privacy exceptions, nonconformities, corrective actions and improvement actions in REG12;

3.1.10 avoid employment-law advice and works council legal commentary inside operational clauses;

3.1.11 avoid duplicate registers, roles, forms, dashboards or HR-specific evidence objects.

4. Policy Statements

4.1 Employee processing inventory and HR processing purposes

4.1.1 [Controller] The Process Owner / Business Owner MUST record each employee processing activity in REG02 before employee PII is collected, generated, imported, used or disclosed.

4.1.2 [Controller] The Process Owner / Business Owner MUST document the employee PII categories, employee population, collection source, processing purpose, system, internal recipient category, external recipient category and retention linkage in REG02 before the processing activity is approved.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST review each new or materially changed employee processing activity in REG02 before the processing activity is approved for operation.

4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST record privacy advice in REG04 before approval of employee processing involving special-category PII, criminal-offence data, background screening, occupational-health data, biometrics, location data, employee monitoring or processing that may materially affect an employee.

4.1.5 [Processor] The Privacy Lead / PIMS Manager MUST record the customer instruction, service purpose, customer employee PII categories and processor role linkage in REG08 before processing customer employee PII as an outsourced HR, payroll, benefits, HRIS, screening or workforce-support service.

4.1.6 [Joint Controller] The Privacy Lead / PIMS Manager MUST record the joint-controller responsibility allocation for employee PII processing in REG08 before the joint employee processing activity begins.

4.2 Employee data collection and employee privacy notices

4.2.1 [Controller] The Process Owner / Business Owner MUST limit employee PII collection to the categories documented in REG02 before recruitment, onboarding, employment administration, benefits administration, payroll operation, screening, monitoring or offboarding collection begins.

4.2.2 [Controller] The Process Owner / Business Owner MUST record the source of employee PII collected from third parties in REG02 before the third-party collection source is used.

4.2.3 [Controller] The Privacy Lead / PIMS Manager MUST maintain an employee privacy notice record in REG07 before employee PII is collected directly or indirectly for a new or materially changed purpose.

4.2.4 [Controller] The Process Owner / Business Owner MUST confirm that the current employee privacy notice recorded in REG07 is available before recruitment collection, onboarding collection, monitoring activation, benefits enrolment, background screening or a material employee processing change.

4.2.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST review the REG07 employee privacy notice record before publication when the notice covers employee monitoring, background screening, special-category PII, criminal-offence data, automated decision-making or a materially changed employee processing purpose.

4.2.6 [Processor] The Vendor / Procurement Owner MUST record employee-facing collection channel responsibilities in REG08 before a processor-operated HR, payroll, HRIS, benefits, screening or outsourced HR service collects employee PII on behalf of a customer.

[... 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 an exception request in REG12 before deviating from any requirement in this policy.

9.1.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of an exception affecting employee monitoring, employee rights handling, background screening, special-category PII, criminal-offence data or high-impact employee processing.

9.1.3 [Conditional] Top Management MUST approve employee privacy exceptions in REG12 before activation when the exception affects high-risk employee processing, employee monitoring, external disclosure, processor reliance or unresolved corrective action.

9.1.4 [All] The Privacy Lead / PIMS Manager MUST assign an expiry date not exceeding 90 days to each employee privacy exception in REG12 before the exception is activated.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST review each employee privacy exception in REG12 within five business days before expiry.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST close or escalate each expired employee privacy exception in REG12 within five business days after expiry.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record a nonconformity in REG12 within five business days when employee PII processing lacks required REG02, REG07, REG08, REG04 or REG06 evidence.

10.1.2 [Conditional] The Incident Response Coordinator MUST record suspected unauthorized employee PII access, disclosure, loss or compromise in REG10 within one business day of identification.

10.1.3 [Controller] The Privacy Lead / PIMS Manager MUST prevent approval of new employee monitoring in REG12 when required REG02, REG04 or REG07 evidence is missing.

10.1.4 [Both] The Vendor / Procurement Owner MUST suspend new employee PII disclosure to an HR vendor in REG08 when required processor, subprocessor, instruction or assistance evidence is missing.

10.1.5 [All] Top Management MUST review repeated employee privacy nonconformities in REG12 when the same category occurs two or more times within a rolling 12-month period.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verify closure evidence in REG12 before closing audit findings involving employee privacy processing, employee notices, employee monitoring, employee rights or HR vendors.

11. Review and Maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy in REG12 at least annually.

11.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST review this policy in REG12 within 30 days of a material change to employee processing, employee monitoring, HR systems, payroll arrangements, HRIS providers, benefits providers, background-screening providers or outsourced HR services.

11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST review proposed material changes to this policy in REG12 before Top Management 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 REG02, REG07 or REG08 within 15 business days after an approved policy change affects employee processing records, employee privacy notices or HR vendor evidence.

11.1.6 [All] The Internal Audit / Compliance Reviewer MUST record review effectiveness observations for this policy in REG12 during the scheduled PIMS internal audit cycle.

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 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 PII11 - PII Accuracy and Quality Policy

12.13 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.14 PII13 - International PII Transfer Policy

12.15 PII14 - PII Security and Access Control Policy

12.16 PII15 - PII Incident and Breach Management Policy

12.17 PII16 - Privacy Training, Awareness and Competence Policy

12.18 PII17 - PIMS Documented Information and Evidence Management Policy

12.19 PII18 - PIMS Monitoring, Audit and Improvement Policy

12.20 PII21 - AI and Automated Decision-Making Privacy Policy, where included in the optional add-on release scope

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 7.5; Clause 8.1** - Mapped to documented employee privacy evidence, operational approval gates, HR processor records, employee notices, monitoring records, exception handling and implementation evidence. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mapped to employee privacy monitoring, metrics, audit evidence, employee monitoring sampling, nonconformity handling, corrective action and improvement. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapped to employee processing purposes, lawful-basis linkage, privacy-risk and DPIA routing, joint-controller allocation and processing records in REG02 and REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].

13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mapped to HR processor contracts, documented instructions, customer employee PII processing, processor assistance and processor records in REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Mapped to employee rights handling, complex rights advice and automated-decision or high-impact processing routing through REG06 and REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Mapped to employee collection limitation, approved internal use, minimization, retention linkage and

retention exception routing. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapped to external employee PII disclosures, data-sharing records, processor disclosure authorization and disclosure-related incident routing. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].

13.2.8 **Annex A.3.14; Annex A.3.25** - Mapped to protection of employee privacy records, employee monitoring log evidence and suspected misuse or compromise of employee monitoring data. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Mapped to lawful, fair, transparent, purpose-limited, minimized, retention-linked and accountable employee PII processing. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].

13.3.2 **Article 6; Article 9; Article 10** - Mapped to lawful-basis linkage, special-category employee PII routing, occupational-health and employment-related sensitive PII routing, and criminal-offence or background-screening data routing. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].

13.3.3 **Article 12; Article 13; Article 14** - Mapped to employee transparency, employee privacy notice records, direct and indirect collection notice triggers, and monitoring notice evidence. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Mapped to employee rights routing, request evidence, complex request advice and automated-decision routing. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mapped to controller governance, joint-controller allocation, HR processor governance, processing records, secure handling, DPIA routing and privacy advisory involvement. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapped to employee purpose specification, collection limitation, minimization, use limitation, retention limitation and disclosure limitation. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mapped to transparency, employee participation, employee rights support, accountability, information security and privacy compliance evidence. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mapped to PII purpose records, collection controls, minimization, retention linkage, disclosure limitation and employee participation or access support. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Mapped to PII-protective workforce lifecycle controls relevant to screening, terms, privacy-breach enforcement linkage and termination or change-of-employment retention review. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Mapped to HR processor evaluation, HR processor monitoring, HR vendor review and service-change evidence in REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Mapped to privacy impact assessment benefits and HR privacy risk or DPIA trigger determination for employee monitoring and high-impact HR processing without duplicating the DPIA method. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Mapped to PII protection, screening, workforce terms, responsibilities after employment change and confidentiality expectations as PII-supporting workforce lifecycle controls. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Mapped to employee monitoring logs, monitoring activities, log-purpose limitation and monitoring evidence review. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].