| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insert Registered Legal Entity Name Here | | | | | | | |
| Document number:<br>PII08 | | | | | Document Title:<br>**Privacy by Design and Default Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>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 6.1.2; Clause 6.1.3 | Both | Supporting | Privacy risk assessment and treatment linkage |
| ISO/IEC 27701:2025 | Clause 6.3; Clause 8.1 | Both | Primary | Planned changes and operational control |
| ISO/IEC 27701:2025 | Clause 7.5 | Both | Supporting | Documented privacy design evidence |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Monitoring and corrective action |
| ISO/IEC 27701:2025 | Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9 | Controller | Supporting | Purposes, PIA trigger and records |
| ISO/IEC 27701:2025 | Annex A.1.4.2; Annex A.1.4.3 | Controller | Primary | Limit collection and processing |
| ISO/IEC 27701:2025 | Annex A.1.4.4; Annex A.1.4.5 | Controller | Supporting | Accuracy and minimization objectives |
| ISO/IEC 27701:2025 | Annex A.1.4.6; Annex A.1.4.7 | Controller | Supporting | De-identification, deletion design and temporary files |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7 | Processor | Supporting | Customer agreement, support and processor records |
| ISO/IEC 27701:2025 | Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4 | Processor | Supporting | Processor design capabilities |
| ISO/IEC 27701:2025 | Annex A.3.27; Annex A.3.29 | Both | Supporting | Development lifecycle and engineering principles |
| GDPR | Article 5(1)(b); Article 5(1)(c); Article 5(2) | Controller | Supporting | Purpose limitation, minimization and accountability |
| GDPR | Article 24 | Controller | Supporting | Controller measures |
| GDPR | Article 25 | Controller | Primary | Data protection by design and default |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 28 | Both | Supporting | Processor instructions and assistance |
| GDPR | Article 30 | Both | Supporting | Processing records |
| GDPR | Article 35 | Controller | Supporting | DPIA trigger linkage |
| ISO/IEC 29100:2020 | Clause 4.7 | Both | Supporting | Privacy controls by design |
| ISO/IEC 29100:2020 | Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6 | Both | Primary | Purpose, collection, minimization and use limitation |
| ISO/IEC 29100:2020 | Clause 5.7; Clause 5.10; Clause 5.12 | Both | Supporting | Accuracy, accountability and compliance |
| ISO/IEC 29151:2022 | Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8 | Both | Primary | PII protection principles and controls |

## 1. Scope

1.1 This policy defines requirements for embedding privacy by design and privacy by default into new and changed PII processing activities, projects, products, services, systems, applications, integrations, procurement activities, and business process changes within the PIMS scope.

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

1.3 Processor and subprocessor obligations apply where the organization designs, configures, changes or operates processing on behalf of a customer, controller or upstream processor under documented instructions.

**1.4 This policy covers:**

1.4.1 privacy requirements at project initiation;

1.4.2 purpose, data minimization and default-setting design controls;

1.4.3 privacy design review before go-live;

1.4.4 change-triggered privacy design review;

1.4.5 procurement privacy-by-design checks;

1.4.6 linkage to privacy risk, DPIA screening and corrective action evidence.

**1.5 This policy does not replace:**

1.5.1 PII03 for processing inventory, purposes, lawful basis and ROPA records;

1.5.2 PII04 for privacy notice content and publication;

1.5.3 PII05 for consent and preference controls;

1.5.4 PII06 for PII principal rights handling;

1.5.5 PII07 for privacy risk assessment and DPIA methodology;

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

1.5.7 PII10 for retention, deletion and disposal execution;

1.5.8 PII11 for accuracy and quality operation;

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

1.5.10 PII13 for international transfer mechanisms;

1.5.11 PII14 for PII security and access control operation;

1.5.12 PII18 for PIMS-wide monitoring, audit, corrective action and improvement governance.

## 2. Purpose

2.1 The purpose of this policy is to ensure that privacy requirements are identified, implemented and evidenced before PII processing begins or materially changes, and that systems and processes are configured by default to limit PII collection, use, exposure, retention dependency, disclosure dependency and identifiability to what is necessary for the documented purpose.

## 3. Objectives

**3.1 The objectives of this policy are to:**

3.1.1 embed privacy requirements into project initiation, design, procurement, change and go-live decisions;

3.1.2 ensure PII processing designs are linked to documented purposes and REG02 processing records;

3.1.3 implement data minimization and privacy-protective default settings before processing begins;

3.1.4 ensure privacy risk and DPIA screening is triggered without duplicating the PII07 methodology;

3.1.5 ensure procurement and processor design requirements are recorded without duplicating PII12 lifecycle governance;

3.1.6 ensure unresolved design issues are escalated through REG12;

3.1.7 maintain audit-ready design evidence in REG02, REG04, REG08 and REG12.

## 4. Policy Statements

### 4.1 Project initiation and privacy requirements

4.1.1 [Both] The Process Owner / Business Owner MUST record a privacy design entry in REG04 before initiating any project, product, service, system, application, integration or business process change that involves PII.

4.1.2 [Both] The Process Owner / Business Owner MUST link each privacy design entry in REG04 to an existing or draft REG02 processing activity before functional requirements are approved.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST record controller privacy-by-design requirements in REG04 before controller functional design approval.

4.1.4 [Processor] The Vendor / Procurement Owner MUST record customer privacy design instructions and contractual design constraints in REG08 before processor service design or material service change approval.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST record advice in REG04 before approval of a high-risk, novel, sensitive, automated, large-scale or materially changed PII design.

4.1.6 [Both] The Information Security Lead MUST record PII security-control dependencies that support the privacy design in REG04 before architecture approval.

### 4.2 Data minimization and privacy-default design

4.2.1 [Controller] The Process Owner / Business Owner MUST document the minimum PII categories, PII principal categories, sources and purposes in REG02 and REG04 before collection or import design approval.

4.2.2 [Both] The System Owner / Application Owner MUST configure default processing settings to the minimum PII collection and processing needed for the documented purpose and record evidence in REG04 before go-live.

4.2.3 [Controller] The Process Owner / Business Owner MUST document optional PII fields, optional processing choices and default-off settings in REG02 and REG04 before user interface, form or workflow approval.

4.2.4 [Both] The System Owner / Application Owner MUST document default privacy exposure settings for views, reports, exports, interfaces and automated workflows in REG04 before go-live.

4.2.5 [Both] The Process Owner / Business Owner MUST document de-identification, pseudonymization, aggregation or non-identifiable processing feasibility in REG04 before approving identifiable PII for testing, analytics, reporting or secondary operational use.

4.2.6 [Both] The System Owner / Application Owner MUST document temporary PII artifact handling, including temporary files, caches, logs or staging records, in REG04 before go-live.

4.2.7 [Both] The Process Owner / Business Owner MUST route design requirements owned by PII10, PII11, PII13 or PII14 to the related policy evidence path in REG04 within five business days of identifying the dependency.

[ ... 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 design exceptions

9.1.1 [Both] The Process Owner / Business Owner MUST request a privacy design exception in REG12 before approving a design or change that cannot meet an applicable privacy design requirement.

9.1.2 [Both] The Privacy Lead / PIMS Manager MUST assess the impact, compensating controls and expiry of each privacy design exception in REG12 within five business days of request.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of a privacy design exception involving high-risk, sensitive, automated, large-scale, disputed or legally material processing.

9.1.4 [All] Top Management MUST approve a privacy design exception affecting high-impact processing, certification scope, unresolved major risk or legal obligation in REG12 before the exception takes effect.

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

9.1.6 [Both] The Privacy Lead / PIMS Manager MUST close or reassess each privacy design exception in REG12 within five business days of expiry.

## 10. Enforcement

### 10.1 Enforcement and nonconformity handling

10.1.1 [Both] The Privacy Lead / PIMS Manager MUST record missing privacy design review, missing minimization evidence, unresolved default-setting failure or unauthorized go-live as a nonconformity in REG12 within five business days of identification.

10.1.2 [Both] The System Owner / Application Owner MUST prevent go-live of a PII-processing system where REG04 privacy design review is incomplete and record the decision in REG12 before go-live.

10.1.3 [Both] The Vendor / Procurement Owner MUST prevent supplier onboarding or contract signature where required REG08 privacy design evidence is absent and record the decision in REG12 before onboarding or signature.

10.1.4 [Both] The Process Owner / Business Owner MUST suspend use of a new or changed PII processing design until REG04 review, REG02 updates and required REG12 exceptions are complete.

10.1.5 [All] Top Management MUST require corrective action in REG12 within 10 business days for repeated, prolonged or high-impact privacy design failure.

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

## 11. Review and Maintenance

### 11.1 Policy and design-control review

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy in REG12 annually and within 30 days of material legal, processing, technology, certification-scope or PIMS control change.

11.1.2 [Both] The Process Owner / Business Owner MUST review active REG02 processing activities for privacy design dependency changes annually and within 30 days of material processing change.

11.1.3 [Both] The System Owner / Application Owner MUST review privacy-default configuration evidence in REG04 annually and within 30 days of material system change.

11.1.4 [Both] The Vendor / Procurement Owner MUST review supplier, processor, subprocessor and third-party privacy design obligations in REG08 before renewal and within 30 days of material relationship change.

11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST review the privacy impact of material policy changes in REG12 before approval.

11.1.6 [All] Top Management MUST approve material changes to this policy in REG12 before publication.

## 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 PII09 - PII Collection, Use, Disclosure and Sharing Policy

12.9 PII10 - PII Retention, Deletion and Disposal Policy

12.10 PII11 - PII Accuracy and Quality Policy

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

12.12 PII13 - International PII Transfer Policy

12.13 PII14 - PII Security and Access Control Policy

12.14 PII17 - PIMS Documented Information and Evidence Management Policy

12.15 PII18 - PIMS Monitoring, Audit and Improvement Policy

## 13. Reference Standards and Frameworks

13.1 This policy is mapped to the following standards and regulations.

13.2 The mapping explains how the policy supports the cited requirements and identifies the internal clauses that implement or support them.

### 13.3 ISO/IEC 27701:2025

13.3.1 **Clause 6.1.2; Clause 6.1.3** - Mapped to privacy risk screening, treatment action linkage, design dependency analysis, escalation and corrective action without duplicating the full privacy risk and DPIA methodology. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.3.2 **Clause 6.3; Clause 8.1** - Mapped to planned privacy changes, project initiation, operational privacy design review, go-live control and material change review. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.3.3 **Clause 7.5** - Mapped to documented privacy design evidence retained in REG02, REG04, REG08 and REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.3.4 **Clause 9.1; Clause 10.2** - Mapped to privacy design metrics, evidence sampling, nonconformity recording, corrective action and effectiveness verification. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.3.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Mapped to documenting processing purposes, processing records, privacy design linkage and privacy risk or DPIA screening triggers for controller processing. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Annex A.1.4.2; Annex A.1.4.3** - Mapped to limiting PII collection and processing through purpose-based minimum data requirements, default-off optional processing and minimum default processing settings. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.3.7 **Annex A.1.4.4; Annex A.1.4.5** - Mapped to accuracy dependency routing, minimization objectives, de-identification feasibility and design evidence for minimizing identifiable PII. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.3.8 **Annex A.1.4.6; Annex A.1.4.7** - Mapped to design-stage identification of de-identification, deletion dependency, temporary PII artifacts and routing to lifecycle controls without duplicating retention or disposal execution. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.3.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapped to processor customer instructions, customer support information, processor design records and customer-authorized service design changes. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.3.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Mapped to processor design capabilities for temporary files, return or disposal dependency, and transmission-control dependency recorded as design evidence without duplicating operational deletion or security-control procedures. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.3.11 **Annex A.3.27; Annex A.3.29** - Mapped to privacy requirements in development lifecycle, engineering principles, PII protection checkpoints and privacy-default configuration evidence. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

### 13.4 GDPR

13.4.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapped to purpose limitation, minimum PII design, processing-record linkage, default minimization, evidence and accountability. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.4.2 **Article 24** - Mapped to controller measures, governance review, exception approval, corrective action and policy maintenance for privacy-by-design implementation. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.4.3 **Article 25** - Mapped to project initiation, design-stage privacy requirements, privacy-default settings, minimization, procurement design checks, go-live review and change-triggered review. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.4.4 **Article 28** - Mapped to processor instructions, processor design support, supplier privacy design evidence and customer-authorized design changes. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.4.5 **Article 30** - Mapped to processing-record linkage, REG02 updates, processing activity design dependencies and processing record evidence. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.4.6 **Article 35** - Mapped to design-stage privacy risk and DPIA screening triggers, high-risk advice and post-implementation checks without duplicating the DPIA methodology. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

### 13.5 ISO/IEC 29100:2020

13.5.1 **Clause 4.7** - Mapped to identifying privacy controls at the design phase, privacy risk linkage and design evidence for control implementation. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.5.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapped to purpose specification, collection limitation, data minimization, limited use and default processing settings. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.5.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Mapped to accuracy dependency routing, accountability evidence, privacy design monitoring, audit and corrective action. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

**13.6 ISO/IEC 29151:2022**

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Mapped to purpose legitimacy, collection limitation, data minimization, use and disclosure limitation, retention dependency, temporary file handling and accuracy dependency design controls. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].