

				Insert Registered Legal Entity Name Here							
Document number: PII04				Document Title: Privacy Notice and Transparency 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

Legal Notice (Copyright & Usage Restrictions)
(C) 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission. Unauthorized use is strictly prohibited and may lead to legal action.
For licensing, contact: info@clarysec.com

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	Notice documented information and operational control
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Notice monitoring and corrective action
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.9	Controller	Supporting	Purpose, lawful-basis linkage, and processing records
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Information and transparency obligations to PII principals
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Joint-controller transparency information
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.3.2	Processor	Supporting	Processor support for controller notice obligations
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparency and accountability
GDPR	Article 12	Controller	Primary	Transparent information and communication
GDPR	Article 13	Controller	Primary	Information where PII is collected from the PII principal
GDPR	Article 14	Controller	Primary	Information where PII is not obtained from the PII principal
GDPR	Article 24	Controller	Supporting	Controller governance measures
GDPR	Article 26	Joint Controller	Supporting	Joint-controller transparency
GDPR	Article 28	Processor	Supporting	Processor assistance and instruction support
GDPR	Article 30	Both	Supporting	Processing-record linkage

ISO/IEC 29100:2020	Clause 5.3; Clause 5.8; Clause 5.10	Both	Supporting	Purpose, transparency, and accountability principles
ISO/IEC 29151:2022	Annex A.9.1; Annex A.9.2	Controller	Supporting	Privacy notice, openness, and transparency controls
ISO/IEC 29184:2020	Clause 5.1; Clause 5.2; Clause 5.3	Controller	Supporting	Online notice objective, provision, and content

1. Scope

1.1 This policy defines requirements for creating, approving, publishing, maintaining, reviewing, and evidencing privacy notices and transparency information for PII processing within the PIMS scope.

1.2 This policy applies to:

- 1.2.1 privacy notices for controller processing activities;
- 1.2.2 transparency information for joint controller processing activities;
- 1.2.3 processor and subprocessor support for controller notice obligations where the organization acts under documented customer or processor instructions;
- 1.2.4 notice content linkage to REG02 processing purposes, lawful-basis references, PII categories, PII principal categories, source categories, recipient categories, retention references, and transfer references;
- 1.2.5 notice publication through digital, physical, contractual, service, product, form, signage, layered, short-form, and just-in-time channels;
- 1.2.6 notice language, version, approval, publication, and review records maintained in REG07;
- 1.2.7 rights-request and privacy contact references linked to REG06;
- 1.2.8 monitoring, exceptions, nonconformities, corrective actions, and improvement evidence maintained in REG12.

1.3 This policy does not define consent capture, consent withdrawal execution, preference management, rights request intake, rights request verification, rights request fulfilment, DPIA methodology, retention execution, international transfer mechanism selection, breach communication, or processor contract negotiation. Those requirements are defined in the related policies listed in Section 12.

1.4 For this policy, a privacy notice means approved external information provided to PII principals or affected audiences describing how PII is processed.

1.5 For this policy, a privacy-significant notice means a notice covering high-risk processing, special category PII, criminal conviction or offence data, child-related processing, employee or monitoring contexts, automated decision-making or profiling, indirect collection at scale, international transfer, joint controller processing, or any notice subject to material legal, regulatory, contractual, or customer scrutiny.

1.6 For this policy, a material notice change means any change to controller identity, contact point, processing purpose, lawful-basis reference, PII category, PII principal category, source category, recipient category, retention reference, transfer reference, rights-request channel, complaint or privacy contact channel, language coverage, publication channel, or processing context that affects the information provided to PII principals.

2. Purpose

2.1 The purpose of this policy is to ensure that PII principals receive clear, current, accessible, and auditable privacy notices before or at the required point in the PII processing lifecycle.

2.2 This policy ensures that privacy notice content is controlled through REG07, aligned to REG02 processing records, supported by REG06 contact and rights-channel references, and reviewed when processing or transparency obligations change.

3. Objectives

3.1 The objectives of this policy are to:

- 3.1.1 establish REG07 as the authoritative evidence object for privacy notice inventory, approval, publication, review, language, and version-control records;

- 3.1.2 ensure each controller privacy notice is linked to current REG02 processing purposes before publication;
- 3.1.3 ensure privacy notices contain approved, audience-appropriate, and externally usable transparency information;
- 3.1.4 define clear approval responsibilities for notice content before publication or collection-channel activation;
- 3.1.5 ensure notices are published through relevant digital and non-digital channels before PII collection or use;
- 3.1.6 maintain controlled notice versions, translated versions, publication evidence, and superseded notice evidence in REG07;
- 3.1.7 ensure notice updates are triggered by material changes to REG02 processing records or transparency obligations;
- 3.1.8 provide processor and subprocessor support for controller notice obligations without duplicating processor governance controls owned by PII12;
- 3.1.9 link privacy notice contact and rights-request references to REG06 without duplicating rights-management controls owned by PII06;
- 3.1.10 avoid creating separate notice approval forms or notice registers outside REG07.

4. Policy Statements

4.1 Notice inventory and processing-purpose linkage

- 4.1.1 [Controller] The Process Owner / Business Owner MUST create a REG07 privacy notice record linked to the relevant REG02 processing activity before launching any new controller PII collection channel, service, form, campaign, product, or feature.
- 4.1.2 [Controller] The Process Owner / Business Owner MUST create a REG07 privacy notice record linked to the relevant REG02 processing activity before using PII obtained from a source other than the PII principal, before first communication with the PII principal, before first disclosure to a third party, or within 20 business days of obtaining the PII, whichever occurs first.
- 4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST maintain the approved REG07 notice field set, including notice ID, owner, linked REG02 records, channel, audience, language, version, effective date, approval status, and publication location, before initial PIMS operation and annually thereafter.
- 4.1.4 [Controller] The Process Owner / Business Owner MUST link each active REG07 notice to every current REG02 processing purpose covered by that notice before notice approval and whenever REG02 is materially changed.
- 4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST record the public-facing joint-controller responsibility summary and contact point in REG07 before joint-controller processing is launched or materially changed.
- 4.1.6 [Processor] The Privacy Lead / PIMS Manager MUST record customer notice-support information in REG07 and link it to REG02 within 10 business days after receiving an approved customer instruction to support a controller notice.
- 4.1.7 [Subprocessor] The Privacy Lead / PIMS Manager MUST record notice-support information requested by the instructing processor in REG07 and link it to REG02 within 10 business days after receiving an approved processor instruction.

4.2 Notice content and transparency information

- 4.2.1 [Controller] The Process Owner / Business Owner MUST include the controller identity and current privacy contact point in REG07 before submitting a privacy notice for approval.

- 4.2.2 [Controller] The Process Owner / Business Owner MUST include each linked REG02 processing purpose and lawful-basis reference in REG07 before submitting a privacy notice for approval.
- 4.2.3 [Controller] The Process Owner / Business Owner MUST include PII categories, PII principal categories, source category where indirect, recipient categories, retention reference, and transfer reference from REG02 in REG07 before submitting a privacy notice for approval.
- 4.2.4 [Controller] The Process Owner / Business Owner MUST include the current REG06 rights-request intake channel and complaint or privacy contact channel in REG07 before submitting a privacy notice for approval.
- 4.2.5 [Controller] The Data Protection Officer / Privacy Advisor MUST record advice in REG07 or REG12 before approval of a privacy-significant notice.
- 4.2.6 [Controller] The Privacy Lead / PIMS Manager MUST verify that the notice content in REG07 is consistent with REG02 before approving the notice for publication.
- 4.2.7 [Controller] The Process Owner / Business Owner MUST record any layered-notice summary, short-form notice, signage wording, or just-in-time notice text in REG07 before publication in the relevant channel.

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

9. Exceptions

9.1 Exception handling

- 9.1.1 [All] The Process Owner / Business Owner MUST record a notice exception request in REG12 before deviating from a requirement in this policy.
- 9.1.2 [Controller] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of any exception affecting notice content, indirect collection timing, privacy-significant processing, or REG06 contact references.
- 9.1.3 [All] Top Management MUST approve any notice exception affecting collection launch, publication timing, high-risk processing, joint-controller transparency, or processor customer commitment in REG12 before the exception takes effect.
- 9.1.4 [All] The Privacy Lead / PIMS Manager MUST record compensating transparency measures, owner, due date, and expiry date in REG12 before a notice exception is approved.
- 9.1.5 [All] The Process Owner / Business Owner MUST close or renew an approved notice exception in REG12 within five business days before the exception expiry date.

10. Enforcement

10.1 Nonconformity and corrective action

- 10.1.1 [All] The Privacy Lead / PIMS Manager MUST record missing, inaccurate, unpublished, unapproved, or obsolete notice evidence as a nonconformity in REG12 within five business days of identification.
- 10.1.2 [Controller] The System Owner / Application Owner MUST block or suspend collection-channel go-live in REG12 when approved REG07 notice publication evidence is missing before go-live.
- 10.1.3 [Controller] The Privacy Lead / PIMS Manager MUST escalate a material inaccurate or misleading notice to the Data Protection Officer / Privacy Advisor and Top Management in REG12 within two business days of confirmation.
- 10.1.4 [Controller] The Process Owner / Business Owner MUST record a corrective action plan in REG12 within 10 business days after assignment of a notice-related nonconformity.

- 10.1.5 [All] The Internal Audit / Compliance Reviewer MUST verify closure evidence for notice-related corrective actions 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 after a material notice, transparency, legal, regulatory, contractual, processing, or certification change.
- 11.1.2 [All] The Data Protection Officer / Privacy Advisor MUST review privacy-significant changes to this policy in REG12 before approval.
- 11.1.3 [All] Top Management MUST approve material changes to this policy in REG12 before publication.
- 11.1.4 [All] The Privacy Lead / PIMS Manager MUST update the REG07 notice field set within 15 business days after approved policy changes that alter notice evidence, approval, publication, review, language, or version-control requirements.
- 11.1.5 [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 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 PII15 - PII Incident and Breach Management Policy
- 12.15 PII17 - PIMS Documented Information and Evidence Management Policy
- 12.16 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 7.5; Clause 8.1** - Mapped to maintaining privacy notice documented information, approval evidence, publication evidence, version records, processor support records, and operational controls before collection or publication. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.5; 4.4.6; 4.6.1; 4.6.2; 4.6.4].

- 13.2.2 **Clause 9.1; Clause 10.2** - Mapped to notice monitoring, REG07 and REG02 reconciliation, mismatch tracking, notice corrective actions, exceptions, enforcement, and effectiveness review. Addressed by clauses [4.5.3; 4.5.4; 4.5.5; 4.5.6; 6.1.2; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.4; 10.1.5].
- 13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.9** - Mapped to REG02 purpose and lawful-basis linkage, controller processing notice records, and records supporting notice evidence. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.2; 4.2.3; 4.2.6; 4.5.1; 4.5.2; 4.5.4].
- 13.2.4 **Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4** - Mapped to determining notice obligations, determining notice information and timing, and providing clear accessible controller information to PII principals. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.5.1; 4.5.2; 4.5.3].
- 13.2.5 **Annex A.1.2.8** - Mapped to recording public-facing joint-controller responsibility and contact information for joint-controller notice transparency. Addressed by clauses [4.1.5; 4.2.1; 4.2.4].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.3.2** - Mapped to processor and subprocessor support for controller notice obligations through customer notice-support information, service processing descriptions, technical publication support, and escalation of conflicting notice-support requests. Addressed by clauses [4.1.6; 4.1.7; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.3 **GDPR**

- 13.3.1 **Article 5(1)(a); Article 5(2)** - Mapped to transparency, evidence-based notice approval, REG07 publication evidence, retained notice versions, reconciliation, corrective action, and accountability metrics. Addressed by clauses [4.1.3; 4.2.6; 4.3.5; 4.4.6; 4.5.4; 4.5.5; 4.5.6; 6.1.2; 8.1.1; 10.1.1].
- 13.3.2 **Article 12** - Mapped to clear, accessible, audience-appropriate, language-controlled notice information and publication through applicable digital and non-digital channels. Addressed by clauses [4.2.4; 4.2.5; 4.2.7; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4].
- 13.3.3 **Article 13** - Mapped to information provided when PII is collected from the PII principal, including controller identity, purposes, lawful-basis references, categories, recipients, retention, transfer references, and rights-channel references. Addressed by clauses [4.1.1; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4].
- 13.3.4 **Article 14** - Mapped to information provided when PII is obtained from a source other than the PII principal, including timing, source category, purposes, categories, recipients, retention, transfer references, and rights-channel references. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.5.2].
- 13.3.5 **Article 24** - Mapped to controller governance measures for notice field sets, privacy advice, approval, publication blocking, review, reconciliation, exception approval, and enforcement. Addressed by clauses [4.1.3; 4.2.5; 4.2.6; 4.3.6; 4.5.3; 4.5.4; 4.5.5; 6.1.1; 6.1.2; 9.1.3; 10.1.2].
- 13.3.6 **Article 26** - Mapped to public-facing joint-controller responsibility and contact information in privacy notices. Addressed by clauses [4.1.5; 4.2.1; 4.2.4].
- 13.3.7 **Article 28** - Mapped to processor and subprocessor support for controller notice obligations, customer notice-support information, and escalation of conflicting support requests. Addressed by clauses [4.1.6; 4.1.7; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 5.1.6].
- 13.3.8 **Article 30** - Mapped to notice linkage with processing records, including purposes, categories, recipients, retention references, transfer references, and processor support records. Addressed by clauses [4.1.4; 4.2.2; 4.2.3; 4.5.4; 4.6.1; 7.1.5].

13.4 **ISO/IEC 29100:2020**

13.4.1 **Clause 5.3; Clause 5.8; Clause 5.10** - Mapped to purpose specification, openness, transparency, notice, and accountability through REG02-linked notice purposes, clear notice content, publication controls, change notice triggers, and evidence-based review. Addressed by clauses [4.1.4; 4.2.2; 4.2.3; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.4; 4.5.6; 8.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.9.1; Annex A.9.2** - Mapped to privacy notice content, plain-language presentation, accessibility, point-of-collection publication, notice update triggers, and openness about privacy practices. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.7; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.5.3].

13.6 ISO/IEC 29184:2020

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3** - Mapped to notice objective, notice provision, clear expression, multilingual presentation, and notice content elements for online or comparable notice channels. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.7; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4].