SRIDA IT PROFESSIONAL REFERENCE PUBLICATION

ISO/IEC 27701:2025

Privacy Information Management System (PIMS)

Requirements, Implementation Guidance & Audit Testing Procedures

DOCUMENT ID	VERSION	STATUS
SRIDA-PIMS-27701-RTP-001	1.0	Final — Approved for Publication

Rajendra Bodda
Chief Information Security Officer (CISO)
Srida IT · 2026

Independent professional guidance.
Not an official ISO or IEC publication.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT



ISO/IEC 27701:2025 — Privacy Information Management System (PIMS)

Requirements, Implementation Guidance & Audit Testing Procedures

SAMPLE

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

Published by Srida IT

SRIDA-PIMS-27701-RTP-001 · Version 1.0 · November 2026

This publication is an independently developed professional guidance document prepared by Srida IT. It is not an official ISO or IEC publication, does not replace the licensed ISO/IEC 27701:2025 standard, and does not confer certification or accreditation.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

Document Information and Control

Field	Value
Document title	ISO/IEC 27701:2025 — Privacy Information Management System (PIMS)
Subtitle	Requirements, Implementation Guidance & Audit Testing Procedures
Document identifier	SRIDA-PIMS-27701-RTP-001
Version	1.0
Status	Final — Approved for Publication
Classification	Srida IT Professional Reference Publication
Author	Rajendra Bodda, Chief Information Security Officer (CISO)
Publisher	Srida IT
Publication year	2026
Issue date	November 2026
Reference standard	ISO/IEC 27701:2025 (standalone PIMS; Clauses 4–10; Annex A Tables A.1–A.3; Annex B)
Related standards	ISO/IEC 27701:2019; ISO/IEC 27001:2022; ISO/IEC 27002:2022; ISO/IEC 29100
Companion publications	SRIDA-ISMS-27001-RTP-001; SRIDA-DPDP-RTP-001; SRIDA-AIMS-42001-RTP-001
Next review	Annually, or on revision of the referenced standards

Version history

Version	Date	Author	Description of change
1.0	November 2026	Rajendra Bodda	First published edition, approved for publication.

Approval

Role	Name	Date
Approved for publication	Rajendra Bodda, Chief Information Security Officer (CISO)	2 November 2026

Distribution

Released for publication by Srida IT. Distribution and use are subject to the permitted-use terms in the Copyright, Legal and Usage Notices.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

Table of Contents

Part I Foundations 16

Chapter 1 Introduction to ISO/IEC 27701:2025 17
Chapter 2 Structure, the 2025 Revision and Certification 21
Chapter 3 Privacy Principles, Roles and the PIMS 25
Chapter 4 ISO/IEC 27701 and Related Standards and Laws 29
Chapter 5 Terminology, Definitions and Abbreviations 33
Chapter 6 How to Use This Manual 37
Chapter 7 Audit Methodology, Evidence and Sampling for Privacy 41

Part II PIMS Requirements (Clauses 4–10) 45

Chapter 8 Clause 4 — Context of the organization 46
Clause 4.1 Understanding the organization and its context 47
Clause 4.2 Understanding the needs and expectations of interested parties 52
Clause 4.3 Determining the scope of the privacy information management system 56
Clause 4.4 Privacy information management system 61
Chapter 9 Clause 5 — Leadership 65
Clause 5.1 Leadership and commitment 66
Clause 5.2 Privacy policy 70
Clause 5.3 Roles, responsibilities and authorities 74
Chapter 10 Clause 6 — Planning 78
Clause 6.1.1 Actions to address risks and opportunities: General 79
Clause 6.1.2 Privacy risk assessment 83
Clause 6.1.3 Privacy risk treatment 88
Clause 6.2 Privacy objectives and planning to achieve them 93
Clause 6.3 Planning of changes 97
Chapter 11 Clause 7 — Support 102
Clause 7.1 Resources 103
Clause 7.2 Competence 107
Clause 7.3 Awareness 111
Clause 7.4 Communication 115
Clause 7.5 Documented information (7.5.1 General, 7.5.2 Creating and updating, 7.5.3 Control of documented information) 119
Chapter 12 Clause 8 — Operation 123
Clause 8.1 Operational planning and control 124
Clause 8.2 Privacy risk assessment 128
Clause 8.3 Privacy risk treatment 132
Chapter 13 Clause 9 — Performance evaluation 136
Clause 9.1 Monitoring, measurement, analysis and evaluation 137
Clause 9.2 Internal audit (9.2.1 General, 9.2.2 Internal audit programme) 141
Clause 9.3 Management review (9.3.1 General, 9.3.2 Management review inputs, 9.3.3 Management review results) 145
Chapter 14 Clause 10 — Improvement 149
Clause 10.1 Continual improvement 150
Clause 10.2 Nonconformity and corrective action 154

Part III Annex A Controls 158

Chapter 15 A.1 Additional controls for PII controllers (Table A.1) 159
A.1.2.2 Identify and document purpose 160

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

A.1.2.3 Identify lawful basis 165
A.1.2.4 Determine when and how consent is to be obtained 170
A.1.2.5 Obtain and record consent 174
A.1.2.6 Privacy impact assessment 178
A.1.2.7 Contracts with PII processors 183
A.1.2.8 Joint PII controller 188
A.1.2.9 Records related to processing PII 192
A.1.3.2 Determining and fulfilling obligations to PII principals 196
A.1.3.3 Determining information for PII principals 201
A.1.3.4 Providing information to PII principals 205
A.1.3.5 Providing mechanism to modify or withdraw consent 209
A.1.3.6 Providing mechanism to object to PII processing 213
A.1.3.7 Access, correction or erasure 217
A.1.3.8 PII controllers' obligations to inform third parties 222
A.1.3.9 Providing copy of PII processed 226
A.1.3.10 Handling requests 230
A.1.3.11 Automated decision making 235
A.1.4.2 Limit collection 240
A.1.4.3 Limit processing 245
A.1.4.4 Accuracy and quality 250
A.1.4.5 PII minimization objectives 254
A.1.4.6 PII de-identification and deletion at the end of processing 259
A.1.4.7 Temporary files 264
A.1.4.8 Retention 268
A.1.4.9 Disposal 272
A.1.4.10 PII transmission controls 276
A.1.5.2 Identify basis for PII transfer between jurisdictions 280
A.1.5.3 Countries and international organizations to which PII can be transferred 285
A.1.5.4 Records of transfer of PII 289
A.1.5.5 Records of PII disclosure to third parties 293

Chapter 16 A.2 Additional controls for PII processors (Table A.2) 297

A.2.2.2 Customer agreement 298
A.2.2.3 Organization's purposes 303
A.2.2.4 Marketing and advertising use 308
A.2.2.5 Infringing instruction 312
A.2.2.6 Customer obligations 316
A.2.2.7 Records related to processing PII 320
A.2.3.2 Obligations to PII principals 324
A.2.4.2 Temporary files 329
A.2.4.3 Return, transfer or disposal of PII 334
A.2.4.4 PII transmission controls 339
A.2.5.2 Basis for PII transfer between jurisdictions 344
A.2.5.3 Countries and international organizations to which PII can be transferred 349
A.2.5.4 Records of PII disclosure to third parties 353
A.2.5.5 Notification of PII disclosure requests 357
A.2.5.6 Legally binding PII disclosures 361
A.2.5.7 Disclosure of subcontractors used to process PII 365
A.2.5.8 Engagement of a subcontractor to process PII 369
A.2.5.9 Change of subcontractor to process PII 373

Chapter 17 A.3 Information security controls for PII controllers and processors (Table A.3) 377

A.3.3 Policies for information security 379
A.3.4 Information security roles and responsibilities 383
A.3.5 Classification of information 387

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

CHAPTER 1

Introduction to ISO/IEC 27701:2025

Almost every organisation processes personal information. Customer records, employee files, patient histories, call recordings, device identifiers, location trails, payment references and support tickets all contain information that relates to identifiable people. That information is collected through websites and mobile applications, shared with payroll bureaux and cloud platforms, analysed for marketing and fraud screening, and retained in backups long after the original purpose has faded. Each of these steps creates obligations towards the people concerned, and each is now regulated in a growing number of jurisdictions.

ISO/IEC 27701 is the international management system standard for privacy. Its 2025 edition specifies requirements for establishing, implementing, maintaining and continually improving a **privacy information management system** (PIMS), together with a catalogue of controls for organisations acting as PII controllers, PII processors, or both. This chapter explains why a management-system approach to privacy is useful, what the standard covers and does not cover, who should use it, and how this manual is intended to support implementers and auditors.

> **Edition status of this manual**
>
> This manual was prepared without access to the licensed text of ISO/IEC 27701:2025. Clause structure follows the ISO Harmonized Structure; Annex A identifiers are taken from secondary public sources, and control titles are carried forward from the 2019 edition and from ISO/IEC 27002:2022. Every 2025-specific identifier, title, count and transition fact is therefore marked and must be checked against the purchased standard before the manual is used for certification-grade work.

1.1 Why a privacy information management system

Privacy failures rarely arise from the absence of a single control. They arise from systemic weaknesses: nobody knows which systems hold personal information; purposes are never written down, so new uses creep in unnoticed; consent is collected in one channel and ignored in another; a supplier is engaged without anyone checking what it does with the data; retention schedules exist on paper but are never executed; a data-subject request is answered late because no one owns the queue. These are management failures, and they recur unless the organisation has a system for deciding, assigning, doing, checking and improving.

A management system supplies that discipline. It requires the organisation to understand its context and the expectations of interested parties, to set a policy and objectives, to assess risk and choose treatments, to resource and train people, to operate defined processes, to measure and audit what happens, and to correct and improve. Applied to privacy, the same cycle forces explicit answers to questions that are often left implicit:

- **In which role does the organisation process each category of PII?** As a controller deciding purposes and means, as a processor acting on a customer's instructions, or as both in different services.
- **Which laws, contracts and commitments apply?** Including sector rules, customer agreements, and the privacy notices the organisation has itself published.
- **What could go wrong for the people concerned?** Not only for the organisation's reputation or revenue, but for the individuals whose information is processed.
- **Which controls are applied, which are excluded, and why?** Recorded in a Statement of Applicability that an auditor can test.
- **How does the organisation know the controls work?** Through monitoring, internal audit and management review rather than assertion.

1.2 Privacy is not the same as information security

Information security protects the confidentiality, integrity and availability of information assets. Privacy protection includes those objectives but goes further. An organisation can hold personal information with excellent encryption and access control and still breach privacy expectations, because it collected more than it needed, used the information for an undisclosed purpose, kept it indefinitely, shared it with an advertising partner, or refused to let the individual see or correct it. Conversely, some privacy obligations, such as honouring an erasure request, can conflict with security practices such as immutable logging and long-term backup.

Table 1-1. Information security and privacy perspectives compared

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

Dimension	Information security perspective	Privacy perspective
Primary concern	Protecting information assets of value to the organisation	Protecting individuals whose information is processed, and meeting obligations owed to them
Who is harmed	Mainly the organisation (loss, disruption, liability)	Mainly the PII principal (discrimination, financial loss, distress, loss of autonomy), then the organisation
Key questions	Who can access it? Is it intact? Is it available?	Should we hold it at all? For what purpose? On what basis? For how long? Who else receives it? Can the person exercise their rights?
Typical failure	Unauthorised access, tampering, outage	Over-collection, function creep, opaque sharing, excessive retention, ignored requests, unlawful transfer
Legitimate processing	Any authorised use is acceptable	Authorised use may still be unlawful or unfair if it exceeds the stated purpose or basis

ISO/IEC 27701 bridges these perspectives. It retains a set of information security controls that matter particularly when the information is PII (Table A.3 in the 2025 edition), and it adds controls that address the privacy-specific lifecycle: purpose, lawful basis, consent, notices, rights, minimisation, retention, disclosure and transfer (Tables A.1 and A.2).

1.3 What ISO/IEC 27701:2025 is

The 2025 edition, published in October 2025, is a standalone management system standard. Its title is understood to be *Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*. In outline:

- **Clauses 4 to 10** contain the management system requirements, arranged according to the ISO Harmonized Structure used by ISO/IEC 27001:2022, ISO/IEC 42001:2023, ISO 9001 and other management system standards. These are the requirements an organisation must conform to if it claims conformity.
- **Annex A** contains reference controls in three tables: A.1 for PII controllers, A.2 for PII processors, and A.3 for information security controls relevant to both roles. Controls are selected through privacy risk treatment and recorded in a Statement of Applicability.
- **Annex B** provides implementation guidance for the Annex A controls. Guidance is informative and describes ways of implementing controls rather than additional requirements.

SAMPLE

The most significant structural change from the 2019 edition is independence from ISO/IEC 27001. The 2019 edition was written as an extension: an organisation had to operate an ISO/IEC 27001 information security management system (ISMS) and then extend it for privacy. The 2025 edition can be implemented on its own, although many organisations will continue to integrate it with an existing ISMS. Chapter 2 explains the revision in detail.

1.4 What the standard is not

Understanding the limits of ISO/IEC 27701 prevents common misunderstandings in sales, procurement and audit conversations.

- **It is not a law and does not create legal compliance.** Implementing the standard helps an organisation build the processes that data protection laws expect, but conformity with ISO/IEC 27701 does not demonstrate compliance with the EU General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act, 2023 (DPDP Act) or any other law. Legal obligations must be identified and met on their own terms. Chapter 4 returns to this point.
- **It does not decide lawful bases, retention periods or notice wording.** It requires the organisation to determine and document these; the content depends on applicable law, contracts and the organisation's own judgement.
- **It is not a technical specification.** It does not prescribe particular encryption algorithms, consent-management platforms or anonymisation techniques.
- **It does not certify anyone by itself.** Certification is granted by certification bodies, ideally accredited for PIMS certification by a national accreditation body. Srida IT is not a certification body, and this manual does not confer or imply certification.

1.5 Who should use ISO/IEC 27701

The standard is applicable to organisations of every size and sector that process PII, in either or both roles. Typical adopters include:

Table 1-2. Typical adopters and their motivations

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

CONTROL A.1.3.7

Access, correction or erasure

Annex A control · PII controller · applicability per privacy risk treatment & SoA | WP-A1.3.7

1 Control Identification

Attribute	Detail
Control identifier†	A.1.3.7
Control title†	Access, correction or erasure
Annex A table and objective	Table A.1 — Additional controls for PII controllers (Table A.1) › A.1.3 Obligations to PII principals
Applies to	PII controller
Control purpose	To ensure PII principals can access their PII and have it corrected or erased, and that the controller fulfils these requests completely, accurately, securely and within the applicable deadline.
Annex B implementation guidance	ISO/IEC 27701:2025 Annex B, B.1.3.7
Corresponding earlier / source control	ISO/IEC 27701:2019 A.7.3.6
Regulatory touchpoints‡	• EU GDPR Art. 15 (access), Art. 16 (rectification), Art. 17 (erasure, including Art. 17(3) exceptions), Art. 18 (restriction); Art. 12(3) timing • India DPDP Act, 2023 s.11 (right to access information about personal data), s.12 (correction, completion, updating and erasure), s.8(7) (erasure when purpose no longer served or consent withdrawn, subject to legal retention); DPDP Rules 2025 Rule 14 — DPDP obligations largely apply from 13 May 2027
Relevant risks	• Access responses are incomplete because PII in secondary systems, backups, logs, email or processor systems is not searched. • PII is disclosed to an impostor because identity verification is weak, causing a breach. • Corrections are made in one system while inaccurate copies persist elsewhere and continue to drive decisions. • Erasure is recorded as complete but PII remains in replicas, data warehouses, processors or backups without a defined handling rule. • Erasure refusals rely on exceptions that do not apply, or are not explained to the principal.

† ISO/IEC 27701:2025 control identifiers and titles are taken from secondary public sources and the corresponding 2019 / ISO/IEC 27002:2022 titles; verify against the licensed standard. ‡ Indicative touchpoints only; implementing a control does not by itself establish compliance with any law.

CONTROL UNDERSTANDING

2 Control Objective and Intended Outcome

The controller operates a documented, tested process through which principals can request access, correction and erasure; requests are verified proportionately, searched across all systems in which the principal's PII is held (including processors), fulfilled or lawfully refused with reasons within the deadline, and fully evidenced.

3 Control Description

This is the most frequently exercised group of rights and the control most often sampled in certification and regulatory audits; Appendix H uses it for the completed workpaper. Srida IT expects an end-to-end design: intake channels; identity verification proportionate to the sensitivity of the PII; a **PII locator** (a system inventory derived from the record of processing that tells handlers where a principal's PII may reside, including processors); search and extraction; review and redaction of third-party PII and legally privileged material; secure delivery; and closure with evidence.

The content of an access response differs by law. GDPR Art. 15 requires a copy of the PII plus supplementary information (purposes, categories, recipients, retention, source, rights, automated decision-making and transfer safeguards). DPDP s.11 requires a summary of personal data and processing activities and the identities of other Data Fiduciaries and Data Processors with whom it has been shared, rather than a full copy. Correction must flow to every system holding the inaccurate data. Erasure

© 2026 Srida IT · Version 1.0 · Independent guidance, not an official ISO/IEC publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

must address primary systems, derived datasets, processors and recipients (see 1.3.8), and backups under a documented rule — commonly 'beyond use' until natural expiry, with re-application of erasure on any restore. Refusals must cite a specific exception (for example legal retention or legal claims) and inform the principal of complaint routes.

4 Business, Ethical and Security Rationale

Access, correction and erasure give principals visibility and control over their PII and enable them to detect misuse. They are the rights most commonly exercised, most frequently complained about, and most readily tested by regulators through mystery-shopper requests. Weak handling also creates security risk: an access process with poor verification is an attack route for social engineering.

5 Risk and Harm Scenarios Addressed

- A fraudster impersonates a retail bank customer by email and receives a full transaction history because only name and date of birth were checked.
- A health-tech SaaS answers an access request from the production database only, omitting support-ticket attachments and analytics exports that contain the patient's PII.
- An HR-payroll BPO erases a former employee's record in the HR system but the payroll processor and data warehouse retain it with no retention basis.

IMPLEMENTATION

6 Applicability and Scoping

Applicable to every PII controller. Exclusion from the Statement of Applicability is not justifiable where any applicable law grants access, correction or erasure rights, which is almost universal. Specific refusals (for example erasure where retention is legally required) are applied case by case, not by excluding the control. Processors support this control under 2.3.2.

7 Implementation Guidance

1. Publish request channels (web form, email, in-app, branch, phone) and accept requests in any reasonable form; record all requests in a central log (1.3.10).
2. Define proportionate identity verification by risk tier, using information already held and avoiding collection of excessive new identity data; define authorised-representative and nominee handling.
3. Maintain a PII locator derived from the record of processing listing every system, data store, unstructured repository and processor that may hold a principal's PII, with search method and owner.
4. Issue search tasks to system owners and processors with deadlines; collate results and record searches performed, including nil returns.
5. Review outputs: redact third-party PII and privileged or exempt material; prepare the response containing the PII and supplementary information required by each applicable law.
6. For corrections, update the source of truth and propagate to all downstream systems and recipients; add a supplementary statement where completion is requested.
7. For erasure, determine whether an exception applies; if not, erase or anonymise across primary systems, derived datasets and processors, place backups beyond use, and flag for re-erasure on restore.
8. Deliver responses securely (authenticated portal or encrypted channel) and confirm completion to the principal with reasons for any refusal and complaint routes.
9. Test the process at least annually with internal test requests across systems, and report volumes and timeliness to management.

8 Roles and Responsibilities

Role	Responsibility
DPO / Privacy Lead	Owns the procedure, decides refusals and exceptions, and reports performance.
Request Handling Team	Logs, verifies, coordinates searches and prepares responses.
System and Data Owners	Search, extract, correct or erase PII in their systems and confirm completion.
Vendor Manager	Instructs processors and obtains confirmation of search, correction or erasure.
Information Security	Defines verification and secure delivery controls; handles backup erasure rules.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

9 Recommended Documented Information

- Access, correction and erasure procedure with verification tiers (see Appendix F)
- PII locator linked to the record of processing
- Request log and case files with search records
- Redaction guidance and response templates by jurisdiction
- Backup and derived-data erasure rule

ASSESSMENT AND TESTING

10 Audit Testing Procedures

Recommended Srida IT testing methodology; not prescribed by ISO/IEC 27701.

Table 15-15. Audit testing procedures, Control A.1.3.7

Test ID	Method	Testing procedure	Result
TP-A.1.3.7-01	**EXAMINE**	Examine the procedure, verification tiers, response templates and PII locator. Confirm they address access, correction and erasure for each jurisdiction in scope, including DPDP s.11 summary content and GDPR Art. 15 supplementary information.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.1.3.7-02	**RE-PERFORM**	Reconcile the PII locator to the record of processing and to the asset inventory. Identify systems, unstructured repositories (email, file shares, ticketing) and processors holding principal PII that are missing from the locator.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.1.3.7-03	**SAMPLE**	Sample closed access, correction and erasure requests and trace each end to end: receipt date, identity verification against the tier, log entry, search tasks issued to every system on the locator and processors, results including nil returns, redaction, response content, delivery method, closure date and deadline compliance.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.1.3.7-04	**RE-PERFORM**	For a sub-sample of access requests, independently search two or more systems for the principal's PII (with appropriate authorisation) and compare with what was disclosed; record omitted data.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.1.3.7-05	**INSPECT**	For sampled erasure and correction requests, inspect primary systems, the data warehouse and one processor to confirm the change took effect; confirm backups are handled under the documented rule.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.1.3.7-06	**EXAMINE**	Examine all refusals and partial fulfilments in the sample. Confirm the exception cited applies, was approved by the DPO and was explained to the principal with complaint routes.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.1.3.7-07	**OBSERVE**	Submit or observe a test access request through a public channel using a test identity with insufficient verification data. Confirm the handler applies the verification tier and does not disclose PII prematurely.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.1.3.7-08	**EXAMINE**	Examine the latest annual process test and management reporting; confirm defects were corrected.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A

11 Sampling Guidance

Srida IT practice: closed requests in the audit period, stratified by type (access, correction, erasure) and channel: all if 25 or fewer; 25 if 26–250; 40 if more than 250; at least 5 of each type where available, all refusals up to 10, and all requests that exceeded the deadline up to 10. Re-perform independent searches for 3–5 access requests. Sample sizes are Srida IT practice, not an ISO requirement.

12 Interview Questions

Interviewee	Question
Request Handler	Show me how you decided which systems to search for this request and how you confirmed nothing was missed.
Information Security Manager	How would you detect and stop a social-engineering attempt through the access process?

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

Interviewee	Question
DPO / Privacy Lead	Which erasure exceptions do you rely on most often, and who approves them?

13 Technical Verification

- Every sampled request was verified according to its tier before disclosure.
- Searches covered all locator systems and relevant processors.
- Responses contained the content required by each applicable law.
- Corrections and erasures took effect across systems and processors.
- Requests closed within deadline or with lawful, notified extension.

14 Expected Audit Evidence

- Request log extract and sampled case files
- Verification records
- Search task records including nil returns
- Redacted response copies and delivery confirmations
- System and processor confirmations of correction or erasure
- Refusal approvals and principal communications
- Annual process test report

15 Evaluation Criteria

Effective

- Sampled requests complete, verified, accurate and on time; re-performed searches find no omitted PII.
- Erasure and correction propagate to all systems and processors with backup handling documented.

Partially effective

- Process sound but the locator omits a secondary system, or a small number of requests were late without harm.
- Supplementary information incomplete in some responses.

Ineffective

- PII disclosed without adequate verification, or re-performance finds significant omitted PII.
- Erasures recorded as complete while PII remains in active systems.

16 Common Gaps and Nonconformities

- Unstructured data (email, file shares, tickets) excluded from searches.
- No processor search or erasure instruction.
- Backups have no documented erasure rule.
- DPDP s.11 response content (shared-with identities) not addressed.

17 Remediation Guidance

- Extend the PII locator to unstructured repositories and processors; use e-discovery tools where volumes justify.
- Introduce tiered verification using existing authenticated channels.
- Document a backup beyond-use and restore re-erasure rule.
- Add DPDP-specific response templates ahead of 13 May 2027.

18 Monitoring Metrics

- Percentage of requests closed within deadline, by type.
- Number of omissions found in internal tests or re-performance.
- Number of verification failures or misdirected responses.

19 Control Maturity Indicators

Initial	Defined	Managed	Optimised
Requests answered ad hoc from the main system; no log or verification standard.	Documented procedure, verification tiers, PII locator for main systems.	Locator complete including processors and unstructured data; deadlines and quality measured; annual testing.	Automated discovery and orchestration across systems and processors with principal self-service and continuous quality sampling.

20 Related Clauses and Controls

- Clauses 8.1, 9.1, 9.2

© 2026 Srida IT · Version 1.0 · Independent guidance, not an official ISO/IEC publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT

- A.1.2.9, A.1.3.2, A.1.3.8, A.1.3.9, A.1.3.10, A.1.4.4, A.1.4.8, A.1.4.9; processor counterpart A.2.3.2
- ISO/IEC 27001:2022 Annex A 5.17, 5.34, 8.10, 8.13
- ISO/IEC 29100 principles: individual participation and access; accuracy and quality

21 Implementation Example

> An auditor samples 25 closed requests at a 400-employee health-tech SaaS acting as controller for its own patient-app users: 14 access, 4 correction, 7 erasure. All were verified through the authenticated app. Re-performing searches for 3 access requests finds chat transcripts in the support ticketing tool that were not disclosed; the tool is missing from the PII locator. Two erasures left records in the analytics processor because no erasure instruction was sent. Result: partially effective; findings raised against the locator and processor instruction steps (see Appendix H for the completed workpaper).

22 Auditor Workpaper Reference

WP-A1.3.7: use the workpaper template in Appendix G.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27701 · © 2026 Srida IT