Owner: Privacy and Trust Operations
Status: Needs DPCO review
Last reviewed: 2026-05-17
Next review: 2026-06-17

ASIRI NDPA Audit-Readiness Pack

This pack summarizes ASIRI's internal NDPA audit-readiness file for buyer, DPCO, counsel, and auditor review. It is designed to help a reviewer understand the operating records ASIRI maintains for its own processing operations and public platform posture.

ASIRI uses this pack as review-ready evidence. It does not replace legal advice, licensed DPCO verification, Compliance Audit Return support, penetration testing, SOC 2 review, ISO 27001 review, or regulator assessment.

Scope

This pack covers ASIRI's own processing operations and public platform posture:

- Public landing site at asiri.ng, including marketing lead capture, privacy and cookie notices, and public consent evidence capture.
- Authenticated product at app.asiri.ng, including RoPA, lawful basis, consent, DSR, DPIA, breach, cross-border, policy, evidence, reports, and Trust Center modules.
- API at api.asiri.ng, including tenant-authenticated workflow APIs and public marketing consent evidence APIs.
- Cloud posture where currently claimed: AWS af-south-1 as the primary processing region, with documented exceptions for selected AI, analytics, payment, email, and edge services.
- Internal records under docs/compliance/asiri-ndpa-audit-readiness/, including the audit matrix, evidence index, operating procedures, registers, DPIA summaries, and management action plan.

Out of scope: customer-selected integrations where a customer independently chooses the destination service, external DPCO opinions not yet issued, regulator determinations, formal security audit reports not yet completed, and customer-specific deployment evidence outside the ASIRI-owned file.

Readiness Summary

ASIRI maintains a structured NDPA audit-readiness file with a machine-readable control matrix, a human-readable evidence index, operating records, and public claim guardrails. The file is owned by Privacy and Trust Operations and is reviewed monthly until external DPCO review is completed; quarterly review is planned after the external review cycle is established.

Current readiness posture:

Area - Current state - Review note
Governance and DPO accountability - Internal evidence file maintained - Needs DPCO review before external outcome language
DCPMI and CAR posture - Preparation artifacts maintained - Licensed DPCO review still pending
RoPA and lawful basis - Internal records and product workflows documented - Reviewer should sample records and evidence exports
Public consent controls - Public consent banner, preferences, gating, and API evidence work present in the repo - Reviewer should confirm production configuration and retention evidence
DSR and breach procedures - SOP and runbook documented with product workflow references - Reviewer should inspect operating history after live use
DPIA process - Platform, marketing, regulatory intelligence, and Trust Center DPIAs documented - Reviewer should confirm risk decisions and open actions
Retention, training, and access review - Evidence packets prepared with live operating samples and sign-offs still required - Management action plan tracks owner evidence collection

Sub-processors and transfers - Internal register, transfer assessment, and public page alignment documented - DPCO/counsel review pending for exceptions
Public assurance claims - Landing audit blocks risky public claims - Public language must stay bounded to audit-readiness and review-ready evidence

The readiness file distinguishes between implemented internal controls, planned controls, and areas that require DPCO, counsel, auditor, or regulator-facing review before ASIRI may describe an external assurance result.

Evidence Index

The evidence index is maintained in docs/compliance/asiri-ndpa-audit-readiness/evidence-index.md and is backed by audit-matrix.json. The current control set is:

Control ID - Obligation - Status - Core evidence
NDPA-GOV-001 - Governance and DPO accountability - Needs DPCO review - README.md, dpo-semiannual-report-template.md, management-action-plan.md
NDPA-REG-001 - DCPMI registration, CAR readiness, and external filing requirements - Needs DPCO review - auditor-pack.md, management-action-plan.md, dpo-semiannual-report-template.md
NDPA-ROPA-001 - Records of processing activities - Implemented - ropa.md, RoPA API routes, RoPA product pages
NDPA-LB-001 - Lawful basis register and LIA evidence - Implemented - lawful-basis-register.md, lawful-basis API routes, lawful-basis product pages
NDPA-CONSENT-001 - Public consent, cookie, withdrawal, and consent evidence controls - Implemented - dpia-marketing-site.md, consent audit script, consent banner, consent preferences, consent evidence API
NDPA-DSR-001 - Data subject rights intake, verification, response, and evidence - Implemented - dsr-sop.md, DSR API routes, DSR product pages, DSR SLA report
NDPA-DPIA-001 - DPIA process for high-risk processing and new technology - Implemented - Marketing, platform, regulatory intelligence, and Trust Center DPIAs
NDPA-BREACH-001 - Personal-data breach triage, notification assessment, and post-incident review - Implemented - breach-response-runbook.md, breach API routes, breach product pages
NDPA-RET-001 - Retention, deletion, and secure disposal - Needs DPCO review - retention-schedule.md, retention/deletion evidence export, consent expiry, file purge, DSR export expiry
NDPA-SUB-001 - Sub-processor governance and vendor risk - Implemented - subprocessor-register.md, vendor-risk-register.md, public sub-processors page
NDPA-XFER-001 - Cross-border transfer assessment and safeguards - Needs DPCO review - cross-border-transfer-assessment.md, cross-border workflows, privacy page
NDPA-SEC-001 - Security controls for confidentiality, integrity, availability, and auditability - Implemented - dpia-platform.md, encryption ADR, deployment checklist, evidence engine
NDPA-ACCESS-001 - Personnel and privileged access review - Needs DPCO review - access-review-record.md, privileged access evidence request, access workflows, RBAC, auth, SSO, SCIM
NDPA-TRAIN-001 - Staff privacy and security training - Needs DPCO review - training-register.md, training/tabletop evidence request, DSR SOP, breach runbook, team workflows
NDPA-AI-001 - Regulatory intelligence and AI risk controls - Needs DPCO review - dpia-regulatory-intelligence.md, vendor/AI evidence request, AI package docs, copilot readiness workflows
NDPA-AUDIT-001 - Audit-readiness pack, evidence index, management action plan, and public claim boundary - Needs DPCO review - audit-matrix.json, evidence-index.md, auditor-pack.md, management-action-plan.md, NDPA audit script

The landing unit test pipeline runs ndpa-audit-readiness-audit.mjs to confirm required evidence files exist, matrix evidence paths resolve, the review boundary sentence remains present, and public pages avoid unsupported assurance claims.

DPIA Summary

ASIRI maintains DPIA artifacts for the main processing surfaces that affect its own audit-readiness posture:

DPIA - Processing surface - Key risks reviewed - Current follow-up
dpia-marketing-site.md - Public landing site, marketing forms, cookie consent, consent evidence APIs - Consent validity, withdrawal, analytics minimisation, public notice clarity - Confirm production consent logging, retention, and marketing API evidence export
dpia-platform.md - Authenticated product and API - Tenant isolation, role-based access, audit events, encryption, backups, evidence workflow access - Attach production infrastructure diagram and latest access-review export
dpia-regulatory-intelligence.md - AI-assisted regulatory intelligence and readiness workflows - Tokenisation, provider regions, sensitive prompt minimisation, human review, output governance - Confirm active AI provider path, model region, and DPCO/counsel review of transfer posture
dpia-trust-center.md - Public Trust Center and procurement-security disclosures - Overstatement risk, stale evidence, sub-processor transparency, public claim discipline - Keep public copy aligned with the claim guard and external validation boundary

Each DPIA is an internal risk assessment artifact. DPCO, counsel, auditor, and regulator-facing determinations remain outside ASIRI's self-issued control.

Operational Procedures

ASIRI maintains operating records for recurring privacy and security workflows:

- ropa.md: processing activity records for ASIRI-owned operations and customer-facing processing support.
- lawful-basis-register.md: lawful basis mapping for platform, marketing, security, billing, support, and regulatory intelligence activities.
- dsr-sop.md: data subject rights intake, identity verification, response timing, portability, erasure, objection, restriction, and evidence retention steps.
- breach-response-runbook.md: personal-data breach triage, containment, 72-hour notification assessment, communications, remediation, and post-incident review.
- retention-schedule.md: target retention and disposal expectations for account, audit, billing, marketing, support, logs, and backup data.
- dpo-semiannual-report-template.md: management review structure for program status, incidents, DSR metrics, DPIAs, vendors, transfers, and open actions.
- training-register.md: staff privacy and security training record for personnel who handle ASIRI or customer data.

These procedures are intended to make ASIRI review-ready by showing how records are maintained, where evidence is stored, who owns each activity, and which items still require operating history or external review.

Security and Access Controls

The audit-readiness file records the following control posture for reviewer sampling:

Control area - Evidence and status
Tenant isolation - API middleware and authenticated app layout references show tenant-scoped workflow patterns; reviewer should sample implementation and production configuration.
Role-based access - RBAC middleware, auth middleware, identity routes, access review workflow, and evidence request are referenced; first signed production access review remains tracked in the management action plan.
Audit logging - Audit middleware and evidence-engine references are included for sensitive workflow actions and evidence lifecycle events.

Encryption - Field-level encryption ADR, environment typing, and deployment checklist are referenced; reviewer should confirm active production settings.
Cloud region posture - AWS af-south-1 is the primary posture where claimed; exceptions for selected AI, analytics, payment, email, and edge services are documented for review.
Evidence integrity - Evidence index, audit matrix, and landing audit script create a repeatable file-existence and claim-boundary check.
Incident response - Breach runbook and breach product workflows document triage, containment, notification assessment, and post-incident review steps.

ASIRI should not use this section as a substitute for a dedicated penetration test, SOC 2 report, ISO 27001 report, or infrastructure security review.

Sub-processors and Transfers

ASIRI maintains subprocessor-register.md, vendor-risk-register.md, and cross-border-transfer-assessment.md for vendor and transfer review. The public sub-processors page is expected to show purpose, region, transfer safeguard, customer data exposure boundary, and review cadence.

Current register themes:

Vendor category - Review focus - Boundary
Hosting and infrastructure - AWS primary hosting, database, storage, secrets, email, evidence collection, and Bedrock where configured - Customer Data and ASIRI operational data may be processed under configured safeguards
Edge and security - DNS, CDN, edge security, and WAF - Public site traffic and limited request metadata; no intentional customer evidence storage
Payment processing - NGN billing and payment metadata - Billing and payment metadata only, not platform evidence content
Analytics - Product analytics where enabled - Event minimisation required; sensitive content should not be sent
AI-assisted workflows - Drafting, extraction, readiness support, and embeddings - Prompts should be minimised or tokenised; human review remains required
Email delivery - Transactional and notification email - Email address, message metadata, and notification content only

Transfer exceptions and AI/analytics regions remain marked for DPCO or counsel review before ASIRI makes any externally reviewed assurance statement.

Management Action Plan

The management action plan is maintained in management-action-plan.md. Current open actions include:

Action ID - Focus - Owner - Due date
MAP-001 - Complete public-copy claim cleanup and rerun landing unit tests - Marketing Engineering - 2026-05-24
MAP-002 - Select licensed DPCO and schedule CAR/readiness scoping review - Privacy and Trust Operations - 2026-06-07
MAP-003 - Confirm AI, analytics, and backup transfer safeguards with DPCO/counsel - Legal and Privacy - 2026-06-17
MAP-004 - Attach first live retention/deletion run and exception-register evidence - Product Engineering - 2026-06-17
MAP-005 - Run privacy/security training and breach tabletop; store attendance evidence - People Operations - 2026-06-17
MAP-006 - Attach first signed privileged access review export - Security Operations - 2026-06-17
MAP-007 - Reconcile internal vendor register with public subprocessor page fields - Vendor Risk - 2026-05-24
MAP-008 - Attach active AI provider, model region, tokenisation, retention, and human-review evidence - Product and Privacy Engineering - 2026-06-17

Open actions are expected to move into closure evidence only after an owner records the action taken, the evidence location, the review date, and any DPCO or counsel feedback where required.

Review Boundary

This pack supports audit-readiness review. It is not an external audit report, regulator finding, legal opinion, DPCO verification statement, Compliance Audit Return filing confirmation, SOC 2 report, ISO 27001 report, or proof of regulator approval.

External DPCO/auditor validation is still required before ASIRI may claim an externally reviewed compliance outcome.

Any public or buyer-facing use of this pack must retain this boundary. ASIRI may describe the file as an internal audit-readiness pack, evidence index, or review-ready summary, while external validation remains pending.