Security & Privacy Overview

ReadinessIQ is the verification layer for home financing. This document summarizes the app-visible security, privacy, and compliance controls in force today. It is intended for enterprise procurement, InfoSec, and compliance reviewers as a pre-DPA reference. It is not a compliance certification.

Document	Security & Privacy Overview
Version / Date	Live — regenerated July 12, 2026
Owner	security@readinessiq.ai
Scope	Production web application and supporting backend services
Data classification	Confidential — for evaluation use only

At a glance

- SOC 2 Type II — audit in progress. We do not represent SOC 2 as certified until the report is issued.
- GLBA-aligned Safeguards program with encryption in transit (TLS 1.2+) and at rest (AES-256).
- Row-Level Security enforced on every borrower-scoped table; least-privilege service roles.
- NMLS verification of every issuing Loan Officer at onboarding and on a rolling cadence.
- TCPA & E-Sign consent recorded with disclosure version, UTC timestamp, and consumer IP.
- No sale of borrower data. Subprocessors are limited, disclosed, and contractually bound.

1. Data handling

Personal information collected includes identifiers required to verify borrower readiness (name, contact, address, employment, income indicators, and, where required by the workflow, government identifiers and account references). Fields classified as sensitive PII are encrypted at the field level in addition to volume encryption.

2. Hosting & infrastructure

Production hosting	Cloud-hosted edge runtime with regional data plane in the United States
Managed data plane	Postgres-compatible service with automated backups and PITR
Network	TLS 1.2+ end-to-end; HSTS; modern cipher suites only
Isolation	Per-tenant Row-Level Security; separate publishable and privileged keys

3. Encryption

- In transit: TLS 1.2+ for all public endpoints and internal service calls.
- At rest: AES-256 volume encryption on the managed data plane and object storage.
- Field-level: sensitive PII (e.g. SSN, DOB, account numbers) encrypted before persistence.
- Key management: keys held by the managed platform; no long-lived static secrets in source.

4. Access control

- Least-privilege by default. Human access to production is gated by SSO with MFA.
- Row-Level Security policies on every borrower-scoped table; service-role key never shipped to browsers.
- Quarterly access reviews; immediate revocation on role change or departure.
- Admin operations are logged and attributable to a named principal.

5. Application security

- SDLC with mandatory review before production merges; dependency scanning on every build.
- Server-only secrets never exposed to the browser bundle; publishable keys are read-only and RLS-scoped.
- Input validated at trust boundaries (server functions and public API routes).

- Webhooks verified with HMAC and timing-safe comparison before any state change.

6. Monitoring & logging

- Application and edge logs retained for operational and security review.
- Anomaly and error monitoring on server functions and public API routes.
- Consent, verification, and passport-scan events are immutable audit records.

7. Incident response

ReadinessIQ maintains a written Incident Response plan covering detection, triage, containment, eradication, recovery, and post-incident review. Confirmed incidents affecting customer data are notified without undue delay and, at a minimum, within contractually agreed timelines. Contact: security@readinessiq.ai.

8. Business continuity

- Managed data plane with automated backups and point-in-time recovery.
- Stateless application tier deployable to the edge for rapid failover.
- RTO / RPO objectives defined internally and available under NDA.

9. Subprocessors

ReadinessIQ uses a limited set of subprocessors to deliver the service. Each is bound by written data protection terms. A current subprocessor list is available on request.

- Managed backend platform — application, database, auth, storage (US region).
- Edge compute / CDN — application delivery and TLS termination.
- Transactional email provider — service and consent-related notifications.
- Telephony provider — voice and messaging where enabled by the customer.
- Model / AI gateway — natural-language features; no borrower PII used to train third-party models.

10. Data retention & deletion

- Borrower records retained per the lender or partner agreement and applicable law.
- Consent, verification, and audit events retained on an immutable timeline for regulatory review.
- Consumer deletion requests honored per CCPA / applicable rights; audit records may be retained in de-identified form where required by law.

11. Compliance posture

SOC 2 Type II	In progress — not yet issued. No representation of certification.
GLBA Safeguards Rule (16 CFR 314)	Aligned — WISP, encryption, access controls, monitoring.
TCPA / E-Sign	Consent captured with disclosure version, UTC timestamp, and IP.
CCPA / CPRA	Consumer rights honored; no sale of personal information.
GDPR	Standard Contractual Clauses available where processing reaches EU data subjects.
NMLS	Every issuing Loan Officer verified against NMLS Consumer Access.

12. Data Processing Agreement (DPA)

A signed DPA is available on request for customers and prospects under NDA. The DPA incorporates GLBA-aligned Safeguards commitments, breach notification timelines, subprocessor terms, and — where applicable — Standard Contractual Clauses for cross-border transfers.

To request a signed DPA, email security@readinessiq.ai with your entity name and counter-signature contact.

Contacts

Security & incident response	security@readinessiq.ai
Privacy & consumer rights	privacy@readinessiq.ai
Compliance & procurement	compliance@readinessiq.ai
Support	support@readinessiq.ai

Disclaimer

This overview reflects app-visible controls in force as of the generation date shown in the header. It is provided for evaluation only, does not create contractual commitments, and is not a compliance certification. Definitive terms are set by the executed Master Services Agreement and Data Processing Agreement between the parties. A Verified Readiness Passport™ is buyer-readiness verification only and is not a loan approval, commitment, or offer of credit.