SmartPR

SECURITY & TRUST

Built for trust. Designed for regulated work.

Enterprise security, data protection, AI governance, and assurance readiness for organizations using SmartPR.

Server-side RBAC	SSO + SCIM	Audited voice access	SOC 2 readiness

Trust Center **trust.getsmartpr.com**

Prepared for	Customers, security teams, IT, compliance and procurement
Review date	September 2026
Assurance status	SOC 2 readiness program; no certification or attestation claim

SECURITY PROGRAM

1. Security posture at a glance

SmartPR is a multi-tenant regulatory intelligence and workflow platform. Its security model is designed around server-side authorization, workspace isolation, controlled privileged access, auditable operations, protected credentials, and enterprise identity capabilities.

Area	Status	What customers should know
Authentication & sessions	**Implemented**	Supabase Auth with server-side session handling.
Workspace RBAC	**Implemented**	Workspace and enterprise permissions enforced in server-side APIs.
Tenant isolation	**Implemented / verify prod**	Application-layer scoping is in place; production RLS coverage is verified separately.
SSO / SCIM	**Available / verify prod**	Enterprise identity controls exist; live IdP setup is environment-specific.
Phone & voice access	**Implemented**	PIN-gated account access with lockout, short-lived sessions, workspace authorization and audit logging.
Privileged support access	**Implemented**	Reason-bound, time-limited, read-only by default, and audited.
Audit logging	**Implemented**	Sensitive enterprise, admin and voice activity generates audit records.
Secrets & service accounts	**Implemented**	Hash-stored machine credentials with scope, rotation and revocation.
AI governance	**Program in place**	Data minimization and controlled logging; provider terms are verified contractually.
SOC 2	**Readiness only**	Control mapping and evidence framework exist; no report or certification is claimed.

What this means for customers

SmartPR already includes the core application controls expected for enterprise use. The remaining assurance work is primarily production verification, recurring operating evidence, and independent attestation.

ACCESS CONTROL

2. Identity, access, and tenant protection

Enterprise identity

- User authentication is integrated with Supabase Auth and application middleware manages authenticated sessions.
- Enterprise workspaces support SSO configuration and domain-based enforcement controls.
- SCIM 2.0 supports managed user and group lifecycle workflows using scoped service-account credentials.
- MFA and session policy settings are represented in the enterprise security posture; live enforcement is validated at the identity-provider layer.

Authorization and least privilege

- Workspace access is role-based, with Owner, Admin, Member, Viewer, and enterprise permission scopes.
- Sensitive administrative and enterprise APIs enforce authorization server-side rather than relying on UI visibility.
- Service accounts support scopes, expiration, revocation, fingerprints, and last-use tracking.

Tenant isolation

SmartPR scopes operations to a workspace and uses centralized permission checks before workspace data is read or changed. Database row-level security is part of the architecture; complete production RLS coverage is validated as a deployment control.

Privileged support access

- Support access requires an explicit reason and defined duration.
- Read-only is the default support scope.
- Expiration is enforced and support access does not create ordinary workspace membership.
- Grant, use, revoke and expiry-related activity is auditable.

Customer-configurable enterprise controls

SSO / SAML · SCIM provisioning · Group-to-role mapping · Session policy · MFA policy · Enterprise roles · Audit-log access

VOICE CHANNEL

3. Secure phone and voice access

SmartPR provides a voice channel for general regulatory questions and authenticated account access. General requirements can be discussed without account access. Account-specific information and actions require successful PIN verification.

PIN protection

Users create a 6-digit voice PIN. PINs are never stored in plaintext. SmartPR stores a scrypt-derived hash using a unique random salt and verifies the PIN using constant-time comparison.

Brute-force protection

After 5 failed PIN attempts, voice account access is locked for 15 minutes before another verification attempt is permitted.

Short-lived sessions

Successful verification creates an opaque 256-bit bearer token. Only its SHA-256 hash is stored. Voice sessions expire 30 minutes after issuance and can be revoked.

Authorization + audit

Each authenticated request derives the user and workspace server-side, checks resource access and plan entitlements, performs the operation, and records the activity in the voice audit trail.

Controlled voice actions

- Account-changing actions use an explicit confirmation step before execution.
- The platform voice experience can populate structured intake fields under the same application permissions and validation rules as typed intake.
- Voice audit records cover authentication events, session lifecycle, tool calls, denials, lockouts and related security activity.
- The session credential cannot override identity, workspace, role, plan, or authorization scope; those values are derived server-side.

Design principle

Voice is another controlled interface into SmartPR - not a bypass around authorization, validation, or audit controls.

DATA SECURITY

4. Data protection, auditability, and integrations

Auditability

SmartPR records security-relevant administrative, enterprise, and voice events. Secret-like values are redacted before inclusion in audit payloads, and sensitive operations are designed to be traceable.

Credentials and secrets

- Service-account credentials are hash-stored and intended to be shown only at creation or rotation.
- Revoked or expired machine credentials are rejected.
- Webhook signing secrets are protected with AES-256-GCM when application-managed storage is used.
- Outbound webhook integrity can be protected with HMAC-SHA256 signatures.
- Server-side redaction helpers reduce the risk of credentials leaking through logs or API responses.

Current production subprocessors

Provider	Purpose	Typical data category
Supabase	Authentication, PostgreSQL, file storage	Account, workspace, application and evidence data
Railway	Application / worker hosting	Runtime data, logs and environment configuration
xAI	AI model processing and voice integration	Prompt or voice-request context needed for the enabled feature
Stripe	Billing and subscriptions	Billing identifiers and payment-related tokens
Google / Gmail SMTP	Operational notifications	Notification / lead content

Browser-assisted agency automation is under development and is not represented as a generally available production capability in this package.

AI GOVERNANCE

5. AI and customer data governance

SmartPR uses AI to interpret regulatory context, assist with application preparation, support voice-based account interactions, and power selected workflow capabilities. Customer information used in AI-assisted features is treated as confidential application data.

Current engineering principles

- AI routes remain subject to authentication and workspace authorization.
- Operational AI logging is designed to capture metadata without recording raw confidential prompt content.
- Provider credentials remain server-side.
- The platform's internal guidance requires minimizing customer information sent to an AI provider to what is necessary for the operation.
- SmartPR does not operate a first-party foundation-model training pipeline using customer application data.

Enterprise diligence

Contractual commitments regarding model-provider training, retention, deletion, geographic processing, and vendor attestations are validated against the applicable provider configuration and terms during enterprise diligence.

Browser automation status

Browser-assisted agency filing is still in development. SmartPR does not present that workflow as a generally available production security or filing capability.

Questions SmartPR can address during diligence

- Which AI providers are used for the customer's enabled features?
- What data categories are sent to each provider?
- What retention and training terms apply to the contracted API service?
- Can specific features or data flows be restricted for an enterprise deployment?

ASSURANCE

6. Security operations and assurance

Security governance

SmartPR maintains a structured security-control registry and internal workflows for evidence, privileged-access reviews, incidents, risks, and policies. The goal is to demonstrate that security controls operate over time, not merely that security features exist in code.

- Privileged-access review workflow and evidence capture
- Security incident register and incident-response plan
- Security risk register
- Policy register and review dates
- Change/deployment evidence model
- Vulnerability-management process and remediation tracking
- Backup/restore evidence model

SOC 2 status

Readiness, not certification

SmartPR maintains SOC 2 readiness materials and control mappings. SmartPR does not currently claim an issued SOC 2 report, certification, or attestation. Formal SOC 2 assurance requires an independent examination by a licensed CPA firm.

Readiness items being independently verified

- Production database row-level security coverage
- Production identity-provider SSO and MFA enforcement
- Backup retention, recovery capabilities, and restore testing
- GitHub branch protection and required CI security checks
- Vendor SOC/security reports and contractual data-processing terms
- Recurring vulnerability scan evidence and operating cadence

Security diligence resources

- Trust Center: trust.getsmartpr.com
- Security & Trust package
- Technical security questionnaire responses
- Subprocessor and AI data-flow review
- Identity / SSO / SCIM architecture discussion
- Role and permissions matrix
- Audit-log and privileged-access walkthrough
- SOC 2 readiness status and assurance roadmap

Important assurance statement

This document is an informational security overview, not an audit opinion, certification, warranty, or substitute for contractual security terms. Control availability may depend on deployment configuration and customer-selected features. Environment-specific claims are validated during formal diligence.