Security questionnaire, answered

The questions security and procurement teams ask about PSP SignalDesk, answered from how the service runs today.

1. Company and contacts

Who provides the service?	PT Pacific Strategy Partners, Jakarta, with Pacific Strategy Partners, Sydney.
Who is the contact for security and privacy?	security@pspsignaldesk.com for security reports and privacy@pspsignaldesk.com for privacy, with a contact person domiciled in Indonesia.
Is the operator registered?	Yes. Private-scope Electronic System Operator in Indonesia, TDPSE 029810.01/DJAI.PSE/09/2026.

2. Data

What data does the service hold?	The customer's AI register: its AI tools, the answers it gives about them, findings and reports. From systems the customer connects: staff names, sign-in addresses, offices and the apps they use. No records of the customer's own customers are collected.
Who owns the data?	The customer. It is the controller of its register and everything in it.
Who at PSP can see it?	Our team sees sign-up and billing details only. Nothing of a customer's AI tools, answers or results is shown in any admin view, alert or sales material.
How is one customer kept apart from another?	Every request for a register is resolved from the signed-in session, never from an identifier the browser sends.

3. Hosting and location

Where is the service hosted?	On Cloudflare's network, with the platform's processing placed in Jakarta. Records are held in Cloudflare's key-value store; the nightly backup is kept in Cloudflare's Asia-Pacific region.
Where else is data processed?	AI analysis, email delivery and card payments in the United States, under each provider's written terms; Indonesian accounting connections in Indonesia. Every provider is listed with its country.

4. Sign-in and access

How do users sign in?	With a one-time code sent to the work email, or with Google. AI Governance accounts carry no password.

Is there a second factor?	The emailed one-time code is required at each new sign-in. Google sign-in carries the second factor the customer enforces on Google.
Is single sign-on offered?	Google sign-in is offered. SAML or OIDC single sign-on is not offered for sign-in today; Microsoft 365 and Okta connect read-only for the register.
How are sessions managed?	Signed access tokens (HMAC-SHA256) valid 30 minutes, renewed from a secure, HTTP-only cookie valid 30 days.
How are repeated attempts stopped?	Rate limits on sign-up, sign-in codes, plan changes and payments, by address and by connection.
Who administers the platform?	Two administrator accounts. Administrative functions need a separate 30-minute credential issued from a live session.

5. Encryption and secrets

In transit?	TLS on every address, HSTS for one year including subdomains.
At rest?	AES-256-GCM for every record and file on Cloudflare. Connection credentials are encrypted with AES-GCM under a key kept apart from the data; passwords are salted PBKDF2 hashes.
Where are keys and secrets kept?	Only in the platform's runtime settings on Cloudflare, never in code, files or the code repository.

6. Connections

What does each connection read?	All connections are read-only. Microsoft 365: the apps in the tenant, their permissions and the user list. Google Workspace: the staff list, the apps each person has authorised, and Google's audit reports. Okta: the apps, assignments and sign-ins. Slack: its admin and user lists.
How are connections removed?	Disconnecting revokes access at the provider and deletes the stored credential. Closing the account deletes every connection and what it found.

7. AI processing

Which AI provider is used?	Anthropic, under its commercial terms, through a relay placed in Singapore.
Is customer data used to train AI models?	No. Anthropic's commercial terms do not allow training on customer content.
How long does the AI provider keep data?	Inputs and outputs are deleted within 30 days.

What is sent?	Only what each check needs. To check a connected app, only the app's name. A document a customer uploads is read for that session and never stored by PSP.
Does the service make automated decisions about people?	No. It explains and prioritises; anyone may ask for a human review.

8. Operations

How is data backed up?	Every record copied nightly to a private store in Cloudflare's Asia-Pacific region and kept 30 days; transactional stores carry 30-day point-in-time recovery.
What availability is offered?	The service runs on Cloudflare's and Netlify's networks and is operated continuously. Material incidents are notified on the desk. No uptime figure or service level agreement is published.
How is the service monitored?	A daily health report on the night's jobs, backups and deliveries. Sign-in, email delivery and activity logs are kept 12 months.
How are changes released?	Every change is reviewed against its diff before release and recorded with its release identifiers.

9. Incidents and testing

How are breaches notified?	Within three days of confirming a breach of personal data protection, and within 72 hours where the law requires.
Has the service been penetration tested?	The platform's code has been reviewed line by line internally. An independent penetration test has not been commissioned.
Is there a disclosure channel?	Security reports go to security@pspsignaldesk.com, also named in pspsignaldesk.com/.well-known/security.txt.

10. Providers, retention and certification

Which providers handle customer data?	Cloudflare, Anthropic, Resend, Stripe, Netlify, Meta for WhatsApp, ElevenLabs for editorial audio, and Google, Accurate, Kledo and Xero when connected. Thirty days' notice is given before a new provider handles customer data, with the right to object.
How long is data kept?	For the life of the subscription; deleted within three days of closure. Logs 12 months. Invoices and tax records 10 years, as the law requires.
Can individuals exercise their rights?	Yes: access, correction, export, deletion and withdrawal of consent, by writing to privacy@pspsignaldesk.com, answered within three days.
Which certifications apply?	The providers the service runs on publish ISO 27001 and SOC 2 attestations: Cloudflare, Anthropic, Stripe, Resend and Netlify. PSP holds no certification of its own. The product assesses each AI tool's readiness against the NIST AI RMF, ISO/IEC 42001 and the EU AI Act.