Data processing agreement

How PT Pacific Strategy Partners processes personal data on your company's behalf when you use PSP SignalDesk, including AI Governance.

1. This agreement

1.1 This agreement is between the customer named below (the **Customer**) and PT Pacific Strategy Partners, WTC 5, Jl. Jend. Sudirman, Jakarta, Indonesia (**PSP**). It forms part of the PSP SignalDesk terms (version 2.0) and the privacy policy (version 3.5).

1.2 It applies whenever PSP processes personal data on the Customer's behalf. Where it and the terms differ on personal data, this agreement prevails.

2. Roles

2.1 For the Customer's AI register, its findings, reports and answers, and the staff data read from systems the Customer connects, the Customer is the controller (or the business, under United States state privacy laws) and PSP is its processor (or service provider).

2.2 For account, sign-in, billing and support records, PSP is the controller, as its privacy policy sets out.

3. PSP's commitments

PSP will:

3.1 process the personal data only on the Customer's documented instructions: the terms, this agreement and the Customer's use of the service and its settings; and tell the Customer if an instruction appears to break the law;

3.2 make sure everyone who processes it is bound to keep it confidential;

3.3 keep in place the security measures in Annex 1;

3.4 use only the providers in Annex 2, each under written terms that protect the data as this agreement does; give 30 days' notice before a new provider handles the Customer's data, during which the Customer may object;

3.5 help the Customer answer requests from individuals to see, correct, export or delete their data, answering within three days;

3.6 give the Customer the information it reasonably needs for a data protection impact assessment or a regulator's enquiry;

3.7 notify the Customer of a breach of personal data protection within three days of confirming it, and within 72 hours where the law requires, with what is known of its nature, the data and people affected, its likely consequences and the steps taken;

3.8 when the subscription ends, delete the Customer's personal data from its live systems within three days and instruct each provider to delete its copy, keeping only the invoicing and tax records the law requires;

3.9 make available the information the Customer needs to see that PSP meets this agreement, including each provider's published attestations, and answer the Customer's written security

questionnaire once a year.

4. United States state privacy laws

Where the California Consumer Privacy Act or another state's comprehensive privacy law applies, PSP:

4.1 processes the personal data only for the business purposes in Annex 3 and the terms;

4.2 does not sell or share it, and does not keep, use or disclose it outside the direct business relationship with the Customer;

4.3 does not combine it with personal data from other sources, except as those laws allow;

4.4 meets those laws and gives the data the protection they require, and tells the Customer if it can no longer do so; the Customer may then take reasonable steps to stop and remedy any unauthorised use.

5. Transfers

5.1 The personal data is processed in the countries in Annex 2. Each transfer rests on the safeguards in each provider's agreement: their standard contractual clauses and, where held, their Data Privacy Framework certification; and, for accounts in Indonesia, as Article 56 of Law 27 of 2022 on Personal Data Protection provides.

6. AI processing

6.1 PSP sends its AI provider only what each check needs. Under the provider's commercial terms, nothing sent is used to train AI models, and inputs and outputs are deleted within 30 days.

6.2 The service makes no decision with legal or similarly significant effect on any individual, and anyone may ask for a human review at privacy@pspsignaldesk.com.

7. Term and law

7.1 This agreement lasts while PSP processes the Customer's personal data, and is governed by the law that governs the terms.

Signed

For the Customer

Company

Name and title

Signature and date

For PT Pacific Strategy Partners

Name and title

Signature and date

Annex 1. Security measures

1. Encryption in transit: TLS on every address, HSTS for one year including subdomains, a content security policy, frame denial, nosniff, a referrer policy and a permissions policy on every page.
2. Encryption at rest: every record in Cloudflare's key-value store and every object in its storage encrypted with AES-256-GCM. Passwords are salted PBKDF2 hashes; connector keys are stored as hashes; connection credentials are encrypted with AES-GCM under a key kept apart from the data store.
3. Secrets: API keys and webhook secrets are held only in the platform's runtime settings on Cloudflare, never in code or files. Webhooks from Stripe, Resend and WhatsApp are accepted only with a valid signature.
4. Access: sign-in by one-time code to the work email, or by Google. Sessions are signed access tokens (HMAC-SHA256) valid 30 minutes, renewed from a secure, HTTP-only cookie valid 30 days. Every request for a register is resolved from the signed-in session.
5. Limits: rate limits on sign-up, sign-in codes, plan changes, payments and AI requests, by address and by connection. Connection addresses are held for one hour, for these limits only.
6. Administration: two administrator accounts. Administrative functions need a separate 30-minute credential issued from a live session.
7. Connections: Microsoft 365, Google Workspace, Okta and Slack connect read-only. Disconnecting revokes access at the provider and deletes the stored credential.
8. Isolation: the platform runs in Cloudflare's V8 isolates, each unable to read memory outside itself.
9. Backups: every key-value 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.
10. Monitoring and records: a daily health report on the night's jobs, backups and deliveries; sign-in, email delivery and activity logs kept 12 months; every change reviewed against its diff before release and recorded.

Annex 2. Providers

Each processes the Customer's data only as the service needs. Microsoft 365, Google Workspace, Okta and Slack, when the Customer connects them, are the Customer's own providers; the service reads from them and holds the results in the Customer's register.

Provider	Role	Country	Retention
Cloudflare, Inc.	Hosting, runtime and storage	USA; global network	Deleted on account closure; logs 30 days
Anthropic PBC	AI analysis	USA	Inputs and outputs deleted within 30 days; not used for training
Resend, Inc.	Email delivery	USA	30 days
Stripe, Inc.	Payments	USA	Per Stripe's policy
Meta Platforms	WhatsApp Business Platform	USA and Ireland	Held only until delivered

Provider	Role	Country	Retention
ElevenLabs, Inc.	Voice for editorial audio	USA	Editorial scripts only
Google LLC	Drive and Calendar, when connected	USA	Under Limited Use; revoked on disconnect
Accurate, Kledo	Accounting, when connected	Indonesia	Tokens deleted on disconnect
Xero Limited	Accounting, when connected	New Zealand; hosted in the USA	Tokens deleted on disconnect
Netlify, Inc.	Website delivery	USA	Request logs

Annex 3. Details of the processing

Subject and duration	Providing PSP SignalDesk under the terms, for the life of the subscription and until deletion as clause 3.8 sets out.
Nature and purpose	Keeping the Customer's AI register; checking each AI tool against the rules of the markets the Customer serves; finding the AI apps the Customer's staff use through the systems it connects; reports, training and support.
Personal data	Names, roles and work email addresses of the Customer's staff and the owners of its AI tools; from connected systems, staff names, sign-in addresses, offices and the apps each person uses; the answers the Customer gives about its AI tools.
People	The Customer's staff, contractors and the people it names as tool owners.
Special categories	None required by the service.