

PSP SIGNALDESK · PT PACIFIC STRATEGY PARTNERS

PSP SignalDesk Data Protection Statement

How PSP SignalDesk protects the personal data of its subscribers, wherever they are: roles, data, sub-processors, security, retention, rights, incident handling, cross-border transfers, partner administration desks, and the law that applies where you are.

PT Pacific Strategy Partners · Jakarta and Sydney · September 2026

PT Pacific Strategy Partners, Jakarta. Version 3.0, 14 September 2026. Questions about this statement: privacy@pspsignaldesk.com.

1. Who we are and the roles

PSP SignalDesk is a decision-intelligence platform for business leaders across Indonesia and ASEAN, built and operated by PT Pacific Strategy Partners, WTC 5, Jl. Jend. Sudirman, Jakarta, with Pacific Strategy Partners, Sydney. PSP SignalDesk is registered as a private electronic system operator with the Ministry of Communication and Digital Affairs, Tanda Daftar PSE 029810.01/DJAI.PSE/09/2026.

Roles under Law 27/2022 on Personal Data Protection (UU PDP) and Government Regulation 33/2026:

- PSP is the Personal Data Controller of every platform account, under UU PDP in Indonesia and under the data protection law of your own country elsewhere. Subscribers activate the service and accept the platform's Terms and Privacy Policy directly with PSP.
- Where a partner organisation, such as a chamber of commerce or an industry association, makes the platform available to its members, the partner does not provide PSP with its membership database. Members activate directly. The only details a partner passes to PSP are those of people it nominates for program seats, supplied with their consent.
- A partner organisation is the Personal Data Controller of the data it collects through its own channels, and of the program information it sees on its administration desk (section 9), which it uses solely to operate its program.

2. What personal data PSP SignalDesk processes

Who	Personal data	Purpose	Basis
Subscriber	Name, work email, organization, role, language, sector and market preferences, subscription plan and status	Provide and support the subscription	The subscriber's contract with PSP
Subscriber	Analyst conversations, saved decisions, workbook entries, usage counts	Deliver the analysis the subscriber asks for and keep the subscriber's own history	Contract; the subscriber can delete each item at any time

Who	Personal data	Purpose	Basis
Subscriber, optional	WhatsApp number and message text	The WhatsApp assistant	Consent, given when the subscriber links the number; withdrawn by unlinking or replying STOP
Subscriber, optional	Connected business tools: accounting snapshots (Accurate, Kledo, Xero), Google Sheets, Calendar and Drive; uploaded documents	Analysis the subscriber requests on their own figures and documents	Consent, given at connection or upload; withdrawn by disconnecting
Partner officers on an administration desk	Name, email, role	Operate the partner's program	The partner agreement
Everyone	Security and service logs	Security, abuse prevention, service quality	Legitimate interest

Not processed: children's data, voice recordings of subscribers, biometric data, advertising or tracking scripts.

3. Where it is processed: sub-processors

Sub-processor	Role	Country	Retention	Certifications
Cloudflare, Inc.	Hosting, runtime, storage, logs	United States; global network including Jakarta	Deleted on termination; logs 30 days	ISO 27001, 27018, 27701; SOC 2 Type II
Anthropic, PBC	AI analysis for SD Analyst, SignalPulse and document extraction	United States	Inputs and outputs deleted within 30 days; never used to train models	SOC 2 Type II; ISO 27001
Meta Platforms (WhatsApp Business Platform)	WhatsApp message delivery	United States and Ireland	Messages held only until delivered	ISO 27001; SOC 2 Type II
Resend, Inc.	Transactional email: sign-in codes, invoices, briefs	United States	Send logs 30 days	SOC 2 Type II
Stripe, Inc.	Card payments, where a subscriber pays by card	United States	Transaction records as payment law requires	PCI DSS Level 1; SOC 1 and SOC 2

Sub-processor	Role	Country	Retention	Certifications
ElevenLabs, Inc.	Voice generation for editorial audio	United States	Editorial scripts only; no subscriber data	SOC 2 Type II
Netlify, Inc.	Web page hosting	United States	No subscriber data at rest	SOC 2 Type II

Each sub-processor is bound by a data processing agreement under which it acts only on PSP's instruction, applies no training to subscriber content where AI is involved, deletes on request and notifies PSP of any incident.

Not sub-processors: Google, Accurate, Kledo and Xero are services a subscriber chooses to connect, and each is an independent controller of its own system. Connectors a subscriber enables in their own Claude, ChatGPT or Microsoft Copilot account are governed by the subscriber's own agreement with that service.

4. Security measures

- All data is encrypted in transit and at rest.
- Access is by short-lived signed session tokens; administrator functions require a separate administrator session, and a partner's administration desk is limited to the accounts the partner designates.
- Credentials are stored with per-user salted, iterated hashing; repeated failed sign-ins hold the address.
- Connected-tool credentials are encrypted before storage and revoked at the provider when a subscriber disconnects.
- Every activation, sign-in, WhatsApp, analyst and document action is rate-limited.
- The WhatsApp assistant answers linked numbers only, and every inbound message is signature-verified.
- Demo accounts are read-only.
- Security and service events are logged for incident investigation. No third-party analytics or tracking scripts run on the platform.
- Staging is a separate environment with no subscriber data and no outbound email.
- Consent and withdrawal are recorded per subscriber and per purpose, with the notice version and language.
- Closing an account deletes the account record, desk memory, conversations, decisions, workbook, documents and connected-tool credentials on PSP systems within three days, and processors delete within their contractual windows.

A technical description of these controls is available to contracting parties on request under a confidentiality undertaking.

5. Retention

Data class	Retention
Account record and the subscriber's own desk content	Life of the subscription; deleted within three days of closure, or earlier when the subscriber deletes an item
WhatsApp conversation memory	24 hours
Connected-tool data	Cached for the working session only; re-pulled on request; removed on disconnect
Uploaded documents	Deleted at the AI provider after processing, at most 30 days
Support tickets, session requests, survey answers, feedback	Life of the subscription or partner program plus 12 months
Monthly usage counts shown to a partner organisation	16 months
Invoice and payment records	10 years, as Indonesian law requires
Security and service logs	30 days

6. Your rights and how to exercise them

You have the rights that the data protection law of your country gives you. At minimum, wherever you are, we give you: information, access and a copy, correction, deletion, withdrawal of consent, restriction, objection to solely automated decisions, portability and complaint.

- In the portal: correct your profile, delete conversations, decisions and workbook entries, disconnect any connected tool, unlink WhatsApp, and close your account from the Subscription page.
- By email to privacy@pspsignaldesk.com from your account email. A request that reaches a partner organisation is forwarded to PSP the same business day.
- PSP acknowledges within one day and completes access, correction, restriction, withdrawal and deletion on PSP systems within three days.
- WhatsApp: reply STOP or BERHENTI to any message, or unlink in the portal.
- Complaints go to PSP first, then to the supervisory authority named in section 10.

7. If personal data is exposed

A personal data breach is any event in which personal data is lost, altered, disclosed or accessed without authority.

- PSP acts as soon as a breach is suspected: the credential is changed, the access is closed and the facts are established.
- Within three days of confirmation, as UU PDP Article 46 and PP 33/2026 Article 114 require, PSP writes to every affected subscriber by email in the subscriber's language and notifies the supervisory authority. The notice states what data was involved, when and how it happened, what PSP has done, what you should do, and whom to contact.

- Where there is serious public impact, PSP also issues a public notice.
- Sub-processors are bound by contract to tell PSP promptly of any incident on their side, and PSP then follows the same steps.

If you suspect a problem, write to privacy@pspsignaldesk.com at any time and you receive an answer within one day.

8. Cross-border transfers

Subscriber data is processed on Cloudflare's global network and by the sub-processors in section 3 in the United States and Ireland. For subscribers in Indonesia the basis under UU PDP Article 56 is adequate and binding safeguards: a data processing agreement with each sub-processor, no-training terms where AI is involved, instruction-bound processing, deletion on request and incident notification. For subscribers in the European Union, the United Kingdom, Australia and Singapore, transfers to those sub-processors rest on the same agreements, on the sub-processors' standard contractual clauses and, where held, on their EU-US Data Privacy Framework certification. The Privacy Policy tells you this before you activate.

9. Partner administration desks

Where a partner organisation makes the platform available to its members, the officers it designates see, for that partner's members only:

- Email, organization, language, plan, status, and whether the member has chosen a view, chosen an assistant and linked WhatsApp (yes or no only).
- Monthly usage counts: analyst, documents, WhatsApp, site, podcast.
- Support tickets raised by members and their resolution.
- Session and training requests: type, date, format and status.
- Survey results in aggregate, and editorial content published under the partner's program.

Partner officers cannot see:

- Analyst conversations, saved decisions or workbook content.
- Connected-tool data or any credential.
- Uploaded documents.
- WhatsApp numbers or message text.
- Passwords, sign-in codes or session tokens.
- Any data of subscribers outside the partner's program.

The partner uses this information solely to operate its program and does not combine it with its general membership records except to confirm membership. Every administration desk action is logged with the officer's account and the time.

10. Where you are and the law that applies

The same protections in this statement apply to every subscriber, wherever they are. What differs is the law you can rely on and the regulator you can go to.

Indonesia. PT Pacific Strategy Partners is the Personal Data Controller under UU PDP and Government Regulation 33/2026, and PSP SignalDesk is registered as a private-scope Electronic System Operator (PSE Lingkup Privat) under Government Regulation 71/2019, Tanda Daftar PSE 029810.01/DJAI.PSE/09/2026. Rights requests are completed within three days and breaches are notified within three days. The privacy officer is reachable at privacy@pspsignaldesk.com, with a contact person domiciled in Indonesia. The regulator is the Ministry of Communication and Digital Affairs until the Personal Data Protection Authority is formed.

Australia. Pacific Strategy Partners, Sydney, applies the Australian Privacy Principles under the Privacy Act 1988 and the Notifiable Data Breaches scheme, under which an eligible data breach is notified to affected individuals and to the Office of the Australian Information Commissioner. The regulator is the OAIC.

Singapore. Subscribers in Singapore have the rights in the Personal Data Protection Act 2012, including access, correction and withdrawal of consent. The regulator is the Personal Data Protection Commission.

European Union and United Kingdom. Subscribers in the EU and the UK have the rights in the GDPR and the UK GDPR, which this statement meets, with a breach notified to the competent supervisory authority within 72 hours where required. Transfers to our sub-processors rest on their standard contractual clauses and, where held, their Data Privacy Framework certification.

United States and elsewhere. Subscribers in the United States, in the other ASEAN countries, in Japan and in every other country receive the protections in this statement in full. Where your national law gives you a further right, we honour it on request.

Language. For accounts in Indonesia the Bahasa Indonesia text of this statement is the governing text, with English as its equivalent. The French, Dutch, German, Spanish, Chinese and Japanese editions are translations for reading; where they differ from the English, the English applies.

11. Contact

privacy@pspsignaldesk.com for privacy requests, consent withdrawal, human review and complaints. contact@pacificstrategypartners.com for all other matters. PT Pacific Strategy Partners, WTC 5, Jl. Jend. Sudirman, Jakarta. Pacific Strategy Partners, Sydney.