

CONTRACTUAL DOCUMENT

Data Processing Agreement

How PlanSuite handles Customer Data processed on behalf of a customer

Prepared for	Council privacy, security, legal and procurement teams
Prepared by	PlanSuite Pty Ltd ABN 57 691 312 795
Version	1.0 Issued 27 August 2026
Status	External, issued for council privacy, security and legal review
Applies to	Every customer of the PlanSuite Platform, as a Schedule to the Agreement
Document owner	Director, PlanSuite Pty Ltd

1. How this document applies

This Data Processing Agreement forms a Schedule to the Agreement between PlanSuite Pty Ltd (ABN 57 691 312 795) and the Customer. It applies automatically from the date the Customer first accesses the Platform and continues for as long as PlanSuite processes Customer Data. No separate signature is required for it to take effect, and a Customer that requires a counter-signed copy may execute it at Execution below.

Where the Customer's own contract, panel agreement or purchase terms include data protection provisions, those provisions and this document are intended to operate together. Section 15 sets out which prevails if they conflict.

Companion documents

The [Security Information Pack](#) describes the controls behind the commitments made here, and the [Legal Terms and Policies](#) page carries the Terms of Use, Privacy Policy, AI Transparency Policy and Acceptable Use Policy. Where those pages describe a control and this document commits to it, this document governs.

2. Definitions

Terms defined in the Agreement have the same meaning here. In addition:

Agreement	The PlanSuite Terms of Service Agreement together with any Subscription Plan, Schedule, Order Form or incorporated policy.
Customer Data	All information, documents, plans, files, text, images or data uploaded to or entered into the Platform by or on behalf of the Customer, together with the Output generated from it.
Personal Information	Has the meaning given in the Privacy Act 1988 (Cth) and, for a Victorian public sector Customer, the meaning given in the Privacy and Data Protection Act 2014 (Vic).
Data Breach	Unauthorised access to, unauthorised disclosure of, or loss of Customer Data held by PlanSuite or a Subprocessor.
Subprocessor	A third party engaged by PlanSuite that processes Customer Data in order to deliver the Platform. Annex B lists them.

Processing	Any operation performed on Customer Data, including collection, storage, use, transmission, analysis, disclosure and deletion.
ML Processing	The application of an artificial intelligence model to data in order to generate an Output. Section 9 governs it.

3. Roles of the parties

The Customer determines the purposes and means of processing Customer Data and is responsible for the lawfulness of the data it uploads and of the collection notices and consents that sit behind it. PlanSuite processes Customer Data on the Customer's behalf and on its instructions.

Under the Privacy Act 1988 (Cth) the Customer acts as the APP entity accountable for the Personal Information it handles. For a Victorian public sector Customer, PlanSuite acts as a contracted service provider under the Privacy and Data Protection Act 2014 (Vic), and section 14 applies.

The Customer's use of the Platform, its Subscription Plan and this document together constitute the Customer's documented instructions to PlanSuite. Any additional instruction must be given in writing and may be subject to a change in scope or fees where it requires PlanSuite to act outside the ordinary operation of the Platform.

4. Scope and purpose of processing

PlanSuite processes Customer Data solely to provide the Platform and the Services, to support the Customer's use of them, to meet its obligations under the Agreement, and to comply with law. Annex A records the subject matter, duration, nature, purpose, categories of data and categories of individuals.

PlanSuite does not sell Customer Data, does not disclose it for advertising or marketing purposes, and does not use it for any purpose of its own beyond operating and supporting the Platform.

PlanSuite minimises the Personal Information it collects. The Platform is designed around property and planning records rather than individuals, and the Customer controls what it uploads.

5. PlanSuite's processing obligations

PlanSuite will:

1. process Customer Data only on the Customer's documented instructions, and tell the Customer if an instruction appears to require PlanSuite to breach the law;
2. keep Customer Data logically separated by organisation, so a User can reach only the data belonging to their own organisation;
3. maintain the technical and organisational measures in Annex C, and not materially reduce them during the term;
4. restrict access to Customer Data to the personnel who need it to deliver or support the Platform;
5. assist the Customer as set out in section 11;
6. notify the Customer of a Data Breach as set out in section 12; and
7. return or delete Customer Data as set out in section 13.

PlanSuite does not use Customer Data to train, fine-tune or otherwise develop any artificial intelligence model, and does not permit a Subprocessor to do so. Section 9 sets out how this applies to the AI provider.

6. Personnel and confidentiality

Every person with access to Customer Data is bound by a written confidentiality obligation that survives the end of their engagement with PlanSuite. Access is granted on the basis of role and need, is reviewed when a role changes, and is removed when an engagement ends.

PlanSuite is a small organisation and administrative access to production systems is deliberately held by a single director rather than distributed across the team. The Security Information Pack states this openly, including the limits it places on separation of duties.

7. Security measures

PlanSuite maintains the technical and organisational measures set out in Annex C, which are appropriate to the nature of the data processed and to the size of the organisation. They include encryption in transit and at rest, organisation-based access control, private network segmentation, managed backups, centralised logging and continuous error monitoring.

Production infrastructure runs in Amazon Web Services in Sydney, Australia (ap-southeast-2). All Customer Data held by PlanSuite, including the database, uploaded documents, generated reports and application logs, is stored in that region. Section 9 covers AI processing, which is the one exception to in-country processing and is disclosed as such.

8. Subprocessors

The Customer authorises PlanSuite to engage the Subprocessors listed in Annex B. Each is engaged under terms that require it to protect Customer Data to a standard consistent with this document, and PlanSuite remains responsible to the Customer for their performance.

PlanSuite will give the Customer at least 30 days' written notice before adding a new Subprocessor or materially changing the role of an existing one. The Customer may object on reasonable data protection grounds within that period. If the objection cannot be resolved, the Customer may terminate the affected part of the Services without penalty for the remainder of the then-current term.

Not every Subprocessor processes every customer interaction. Which ones apply depends on the modules and integrations the Customer enables, and Annex B records this per provider.

9. Artificial intelligence processing

The Platform uses Google Cloud Vertex AI to analyse property data, planning scheme content and Customer Data in order to generate Output. This is the only processing in which Customer Data leaves PlanSuite's own Australian infrastructure, so it is set out in full here.

Provider	Google Cloud Vertex AI, under a Google Cloud account controlled by PlanSuite
-----------------	--

Models	Gemini models selected by PlanSuite for each task. The current models are listed in the Security Information Pack and may change as Google releases new versions.
Where ML Processing occurs	Google's global endpoint. ML Processing may take place outside Australia, and Google does not offer a data residency guarantee on this endpoint.
Storage and retention	Transient. Customer Data is sent with the request and the Output is returned to PlanSuite's Australian infrastructure, where it is stored. Google's handling of the request itself, including any retention, is governed by the Google Cloud Data Processing Addendum and the Service Specific Terms for Vertex AI.
Training	Google does not use Customer Data submitted through Vertex AI to train or fine-tune any model. This applies to both generally available and pre-release models, under the Training Restriction in the Service Specific Terms.
Logging	PlanSuite does not enable Vertex AI request and response logging.

Regional AI processing

Google publishes ML Processing residency commitments on a per-model and per-region basis. Not every Gemini model carries an Australian commitment, so restricting AI processing to a specific region constrains which models the Platform can use and therefore the quality of the Output. Where a Customer requires region-restricted AI processing, PlanSuite will confirm in writing which models can be used, what the Customer would be giving up, and whether the restriction can be met at all, before any commitment is made.

Output is generated by an AI system and is not a planning decision. The Customer remains responsible for professional review of Output before it is relied on or issued. The AI Transparency Policy on the [Legal Terms and Policies](#) page sets this out in full.

PlanSuite does not operate autonomous agents over Customer Data, does not give the AI provider access to PlanSuite systems, and does not use Customer Data to build a shared model across customers.

10. Disclosure outside Australia

Some Subprocessors process Customer Data outside Australia. Annex B identifies which, and for what purpose. By entering into the Agreement the Customer consents to those disclosures for the purposes described.

Where Australian Privacy Principle 8 or an equivalent obligation applies to the Customer, PlanSuite will provide the information the Customer needs to satisfy itself about the recipient, including the provider, the country, the purpose and the protections in place.

PlanSuite will not introduce a new offshore disclosure of Customer Data without following the notice process in section 8.

11. Assistance to the Customer

PlanSuite will provide reasonable assistance, at no additional charge for requests of ordinary scope, with:

- requests from individuals to access, correct or delete their Personal Information;
- requests made under the Freedom of Information Act 1982 (Vic) or an equivalent regime;
- a privacy impact assessment, security assessment or vendor review the Customer conducts in relation to the Platform;
- the Customer's own reporting obligations, including a Victorian public sector Customer's obligations to the Office of the Victorian Information Commissioner; and
- an enquiry from a regulator concerning the processing of Customer Data.

If PlanSuite receives a request directly from an individual about Customer Data, it will not respond to the substance of the request. It will refer the individual to the Customer and notify the Customer promptly.

If PlanSuite is compelled by law to disclose Customer Data, it will notify the Customer before disclosing unless it is legally prohibited from doing so, and will disclose only what the law requires.

PlanSuite will make available the assurance material it holds, including the Security Information Pack, the Essential Eight alignment and the record of restore validation, and will answer a reasonable annual security questionnaire. PlanSuite does not currently hold ISO 27001 certification, SOC 2 attestation or an independent penetration test report, and says so plainly rather than implying otherwise.

12. Data breach notification

PlanSuite will notify affected Customers within 72 hours of becoming aware of a confirmed Data Breach affecting their Customer Data. This commitment is additional to, and not a substitute for, obligations under the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act 1988 (Cth).

The notification will describe, so far as it is known at the time:

- what happened and when PlanSuite became aware of it;
- the categories of Customer Data affected and, as far as it can be determined, the volume;
- the likely consequences for the Customer and for affected individuals;
- the steps taken to contain and remediate; and
- a named contact for follow-up.

Where the facts are still being established, PlanSuite will notify within the 72 hours with what it knows rather than delaying until the picture is complete, and will provide updates as the investigation progresses.

PlanSuite will cooperate with the Customer's own notification obligations, including notification to the Office of the Australian Information Commissioner and, for a Victorian public sector Customer, to the Office of the Victorian Information Commissioner. PlanSuite will not notify a regulator on the Customer's behalf, nor make a public statement about a Data Breach affecting a Customer, without consulting the Customer first unless the law requires it.

13. Retention, return and deletion

PlanSuite retains Customer Data for as long as the Customer's account is active, and thereafter as set out below.

On termination the Customer may request an export of its Customer Data in a standard format within 30 days of the termination date. After that period PlanSuite may delete the data, and will do so unless retention is required by law.

Deletion extends to backups on the ordinary backup rotation rather than instantly, because backups are taken as point-in-time snapshots. PlanSuite will confirm the

deletion timeframe in writing on request.

Application logs, which carry operational metadata rather than uploaded documents, are retained for 30 days in production and then expire automatically.

14. Victorian public sector customers

Where the Customer is a Victorian public sector organisation, PlanSuite acts as a contracted service provider under the Privacy and Data Protection Act 2014 (Vic) and additionally:

- handles Personal Information in a manner consistent with the Information Privacy Principles in that Act, as they apply to the Customer;
- aligns its security practices to the Victorian Protective Data Security Standards, and publishes its self-assessed position against each standard, including the gaps;
- supports the Customer's Protective Data Security Plan and attestation by supplying the evidence the Customer needs, on the understanding that those submissions are obligations of the Customer's own agency head rather than of PlanSuite; and
- applies the protective markings and handling instructions the Customer specifies in writing for data it uploads.

PlanSuite's self-assessed alignment against each Victorian Protective Data Security Standard, including the standards where it is only partially aligned and why, is available to the Customer on request.

15. Term, variation and precedence

This document takes effect when the Customer first accesses the Platform and continues until PlanSuite no longer holds Customer Data. Sections 6, 10, 12 and 13 survive termination.

PlanSuite may update this document to reflect a change in law, in the Platform or in its Subprocessors. Where a change materially reduces the Customer's protections, PlanSuite will give at least 30 days' written notice and the Customer may terminate the affected part of the Services without penalty if the change cannot be resolved.

If there is an inconsistency between this document and another part of the Agreement on a matter of privacy, data protection or information security, this document prevails. On all other matters the order of precedence in the Terms of Service Agreement applies. Nothing in this document limits a right the Customer has under the Privacy Act 1988 (Cth) or the Privacy and Data Protection Act 2014 (Vic).

16. Governing law and notices

This document is governed by the laws of Victoria, Australia, and the parties submit to the jurisdiction of the courts of that State.

Notices under this document, including a Data Breach notification, are given in writing to the Customer's nominated contact and to PlanSuite at the address below.

Entity	PlanSuite Pty Ltd ABN 57 691 312 795
Contact	support@plansuite.com.au
Document owner	Director, PlanSuite Pty Ltd

Annex A: Details of processing

Subject matter	Provision of the PlanSuite Platform: property and planning data lookup, AI-assisted planning assessment and report generation, and chat.
Duration	The term of the Agreement, plus the retention period in section 13.
Nature of processing	Collection, storage, structuring, analysis, generation of Output, transmission to Subprocessors as described in Annex B, and deletion.
Purpose	To deliver the Platform and Services to the Customer and to support the Customer's use of them.
Categories of data	Property and planning records; documents the Customer uploads, which may include planning applications, plans, permits, titles, correspondence and site photographs; user account records; usage and audit records; support correspondence; and billing records.

Categories of individuals	The Customer's staff who use the Platform; individuals named in documents the Customer uploads, such as applicants, objectors, consultants and property owners; and, where a Customer enables the public portal, members of the public who use it.
Sensitive information	The Platform is not designed to process sensitive information as defined in the Privacy Act 1988 (Cth), and the Customer should not upload it. Where it appears incidentally in an uploaded document it is handled under the same controls as all other Customer Data.

Annex B: Subprocessors

For each provider the table records where Customer Data is processed, where it is stored, and from where PlanSuite personnel can access it. A provider marked as not storing Customer Data receives it only for the duration of the request.

The same register appears as section 7 of the [Security Information Pack](#). Both are generated from one source, so a change reaches every published copy at once.

Provider	Purpose	Processed in	Stored in	Accessible from
Amazon Web Services	Cloud hosting, database, document storage and application logs	Sydney, Australia	Sydney, Australia	Australia
Google Cloud Vertex AI	AI analysis of property data, planning scheme content and user inputs. Not used for model training.	Global endpoint; may occur outside Australia	Not stored	Australia
Google Maps Platform	Map display, aerial imagery, Street View imagery of the property, and address search	United States	Not stored	Australia
Victorian Government APIs	Official planning and property data (VicPlan, Vicmap, Victorian GeoServer)	Victoria, Australia	Not stored	Australia

Provider	Purpose	Processed in	Stored in	Accessible from
Nearmap	Optional high-resolution aerial imagery, enabled per organisation under the council's own Nearmap licence	Australia	Not stored	Australia
Postmark	Transactional email delivery	United States	United States	Australia
Intercom	In-product support messaging	United States	United States	Australia
Stripe	Subscription billing. Card details are captured by Stripe directly and are not held by PlanSuite.	United States	United States	Australia
Sentry	Application error monitoring. Session replay is captured only when an error occurs, with all text masked and all media blocked.	Germany, European Union	Germany, European Union	Australia
HubSpot	Customer relationship management for account and organisation contact records	United States	United States	Australia
Slack	Internal operational and service notifications to PlanSuite staff	United States	United States	Australia

Scope of each provider

Documents the Customer uploads, the reports generated from them and the planning data behind them are held only by Amazon Web Services in Sydney. The remaining providers receive a narrower slice: account and contact records, support messages, billing records, error diagnostics, or the content of a single AI request. Nearmap applies only where the Customer supplies its own licence, and Slack carries operational notifications to PlanSuite staff rather than Customer Data as such.

Annex C: Technical and organisational security measures

Encryption in transit	TLS 1.2 minimum, TLS 1.3 supported, for all connections to the Platform and to Subprocessors.
Encryption at rest	AES-256 for the database, document storage and backups, using managed keys.
Access control	Organisation-based separation of Customer Data, role-based permissions, and optional single sign-on through the Customer's own identity provider.
Administrative access	Restricted to a single director. Production administration is not delegated.
Network	Application and database in private subnets with security group segmentation. The database is not publicly accessible.
Platform	Managed container platform with no general-purpose operating system exposed. Infrastructure defined as version-controlled code, with baselines reapplied on each deployment.
Backups	Managed automated backups with point-in-time recovery, a measured recovery point objective of approximately five minutes, and restore validation on a fixed cadence with recorded results.
Logging and monitoring	Centralised application logging with 30 day production retention, continuous error monitoring, and alerting on defined thresholds.
Vulnerability management	Automated dependency scanning with patches raised on CVE publication, plus secret scanning and push protection on the source repository.
Known limitations	No security information and event management correlation, no independent penetration test, no static application security testing, and a single availability zone database that recovers by restore rather than failover. These are disclosed rather than described as planned controls.

Why the limitations are listed

A council's security review is only useful if the vendor's disclosure is complete. PlanSuite states the controls it does not have alongside the ones it does, so a reviewer can weigh the actual position rather than discover a gap later.

Execution

This document applies as a Schedule to the Agreement without signature. A Customer that requires a counter-signed copy may execute below and return it to PlanSuite.

PlanSuite Pty Ltd

ABN 57 691 312 795

Signature

Name and position

Date

Customer

Organisation and ABN

Signature

Name and position

Date