

Security & Compliance

Security & Compliance Overview

How PlanEase keeps Queensland council and applicant data secure, private, and hosted in Australia. Prepared for vendor evaluation.

Reviewed 2026-07-20

Confidential: prepared for evaluation. Indicative self-assessment, not an independent certification.

1.0 Executive summary

PlanEase is an Australian SaaS platform for managing development-application (DA) conditions in the Queensland planning system. All customer data is hosted in Australia on Amazon Web Services (Sydney), encrypted in transit and at rest, with each tenant's data isolated by server-enforced access control on every request.

This document summarises our security controls, sub-processors, availability, and the governance posture a council procurement team typically assesses. Detailed documentation (privacy policy, sub-processor register, incident-response plan, and a data processing agreement) is available to prospective councils on request.

2.0 Data residency & encryption

- Hosted entirely in **AWS ap-southeast-2 (Sydney)**. AWS holds a current ISO/IEC 27001 certification for the infrastructure layer.
- Encrypted **at rest** (S3 server-side encryption, DynamoDB encryption) and **in transit** (TLS 1.2+ with HSTS).
- The only data received outside Australia is inbound email (an AWS SES regional constraint) and optional Microsoft single sign-on identity.

3.0 Access control & tenant isolation

Every read and write passes through a single, centrally-enforced authorisation check before any data is returned. A caller can only ever reach data their identity is explicitly entitled to; a mismatch returns zero records. Isolation is enforced in server-side code and AWS configuration, not in the browser.

- Role-based access (super-admin, admin, contributor, viewer), with company admins scoped to their own company.
- Sign-in via AWS Cognito and optional Microsoft single sign-on; least-privilege IAM across all services.
- Production and non-production run as fully separate environments (separate data stores and identity pools).

4.0 Sub-processors

Third parties that process data on PlanEase's behalf, with the region in which they process it:

SUB-PROCESSOR	PURPOSE	REGION
Amazon Web Services	Hosting, storage, database, AI, email, authentication	Australia (Sydney, ap-southeast-2)
Microsoft (Entra ID)	Optional single sign-on	Global (Microsoft)
PostHog	Product usage analytics	United States
Amazon SES (inbound)	Inbound project email receipt	United States (us-east-1)

5.0 Availability & resilience

- Target monthly uptime of **99.5%**, with a live public status page at **status.planease.net**.
- Continuous backups: DynamoDB point-in-time recovery across 27 tables (35-day window) and S3 object versioning.
- Audit and access logging via AWS CloudTrail, API Gateway access logs, and an in-application audit trail.

6.0 Compliance posture & roadmap

Live	
Application-security hardening	20+ fixes (access control, tenant binding, SSRF, email authentication) shipped to production.
Australian data residency	Hosted in AWS Sydney; encrypted at rest and in transit (TLS/HSTS).

Tenant isolation	Enforced server-side on every request; Cognito + Microsoft SSO sign-in.
Continuous backups & audit logging	Point-in-time recovery across 27 tables, CloudTrail, API access logs.
Public Privacy Policy	Live and aligned to the Australian Privacy Principles.
Public status page & uptime monitoring	Live uptime monitoring of the app, API, and website, with a public status page at status.planease.net .
Sub-processor register	Every third party, region and purpose.
Tenant-isolation statement	How each council's data is kept isolated from every other tenant.
Data retention & deletion policy	Retention periods set; data frozen on offboarding, deleted on written request.
Incident Response & data-breach plan	Aligned to the Notifiable Data Breaches scheme; operational.
In progress	
Data Processing Agreement	Binds PlanEase under the Qld Information Privacy Act.
SLA & disaster-recovery commitments	99.5% uptime; near-zero data-loss recovery (PITR); 4-hour recovery validated by a restore drill. Off-region backup remains.
Roadmap	
ISO 27001	Roadmap drafted; certification decision pending.
Customer-facing exportable audit trail	For councils' Public Records obligations.
Independent penetration test	External, on an annual cadence.
WCAG 2.1 AA accessibility audit	Leading to a published conformance statement.

7.0 Privacy & legal

- Public Privacy Policy aligned to the Australian Privacy Principles (planease.net/privacy).

- When engaged by a Queensland council, PlanEase is bound as a contracted service provider under the Information Privacy Act 2009 (Qld).
- Incident-response and data-breach plan aligned to the Notifiable Data Breaches scheme; a data processing agreement is available for council contracts.

8.0 Contact

Security and compliance enquiries: **support@planease.net**.

This overview is an indicative self-assessment of PlanEase's posture on the evidence to date. It is not an independent certification, audit, or legal advice. Reviewed 2026-07-20.

Security & Compliance

Security & Compliance Overview

PlanEase Pty Ltd

ABN 81 694 215 506

support@planease.net

planease.net

