Privacy & Security Fact Sheet

BIDLOGIQ

Your Data, Protected and Empowered.

At BIDLOGIQ, we are committed to providing you with powerful AI-driven tender management services built on a foundation of trust, transparency, and robust security. This document outlines our approach to managing and protecting your information in line with the highest standards.

Our Core Commitments

Privacy by Design	Robust Security	Data Ownership	Transparent AI
We adhere to the Australian Privacy Principles (APPs). We only collect the information necessary to provide and improve our services to you.	We leverage the enterprise-grade infrastructure of **Google Cloud Platform**, with data encrypted both in transit (TLS 1.2+) and at rest.	You retain **100% ownership** of your data at all times. Our platform is designed to give you maximum control over your documents and information.	Our AI works for you. Your data is **never used to train AI models** and is never shared or used to generate responses for other clients.

What Information We Handle

We handle two main categories of information to provide our service:

- **Personal Information:** To manage your account and provide quality service, we collect basic identifiers like **names, business addresses, email addresses, and phone numbers**. We do not collect or process sensitive information (e.g., racial origin, political opinions, health information).
- **Client-Provided Company Data:** This includes the tender documents, CVs, and other company files you provide for processing. This data is the core of our service, used to generate capability reports, draft responses, and perform reviews.

We do not store or process your financial data.

Secure & Ethical AI, Powered by Google Gemini

Our AI-powered features are a key part of the value we provide. We understand that using AI with your business-critical data requires absolute confidence in the process.

- **Secure Processing:** Full documents are processed in memory to retrieve context. Required data is then sent securely to the Google Gemini API for analysis.
- **Your Data is Not Used for Training:** As a paid, enterprise-grade service, Google **does not use your data to train their models**. This is a key term of our agreement with Google.
- **Complete Isolation:** Each request to the AI is processed independently. Your data is never exposed to or used in generating responses for any other BIDLOGIQ client.

Microsoft SharePoint Integration: You Control Your Documents

For maximum security and control, we offer seamless integration with your existing Microsoft SharePoint environment.

- **Your Documents Stay in Your Tenant:** Source documents and files remain within your SharePoint, governed by your organization's security and access policies. BIDLOGIQ reads these files for processing but **does not store a separate copy** on our systems.
- **Generated Files Stored in Your SharePoint:** Any files generated by BIDLOGIQ (e.g., capability reports, draft responses) are also stored directly in your secure SharePoint tenant.
- **Minimal Data Footprint:** Only essential metadata related to processing is stored in our secure Firebase environment, ensuring you retain primary control over your intellectual property.

Questions?

If you have any queries about our Privacy Policy or security posture, please contact us.

Email: support@bidlogiq.ai
Phone: +61 (0)7 2143 6035

Security Architecture & Operational Controls

A Technical Overview for Your IT and Security Teams.

Hosting, Sovereignty & Data Portability

FEATURE	BIDLOGIQ Implementation
HOSTING	**Google Cloud Platform (GCP)** and its **Firebase** services.
DATA CENTRE LOCATION	All core services and metadata are hosted in the australia-southeast1 (Sydney) region. The generative AI endpoint utilizes Global infrastructure for maximum quality. This is configurable by request to any supported region (including Sydney); however, restricting processing to specific regions may limit access to the latest high-fidelity models. As regional support expands, these options will automatically increase. See available regions or contact us for further information:
REDUNDANCY	High availability and data redundancy are built-in via Google Cloud's native infrastructure.
DATA OWNERSHIP	**You retain full ownership** of all your data.
DATA EXPORT	Data can be exported upon request. If using SharePoint integration, your data already resides in your environment.

Data Protection & Encryption

FEATURE	BIDLOGIQ Implementation
DATA IN TRANSIT	All external communications are encrypted using **HTTPS/TLS 1.2+**.
DATA AT REST	All stored data uses **User-Controlled Encryption**. Keys are derived from your password and never persisted on our servers, ensuring only you have access to your documents. Secure recovery keys prevent data loss.
INTERNAL ENCRYPTION	Communication between our internal microservices is secured and authenticated.
DATA LOSS PREVENTION	Google Cloud provides infrastructure redundancy. Our daily backups and 60-day retention policy prevent indefinite storage, and usage limits prevent accidental mass data creation.

Access Control & Identity Management

FEATURE	BIDLOGIQ Implementation
AUTHENTICATION	All internal and external APIs are protected via **Firebase ID token authentication**.
MULTI-FACTOR AUTH (MFA)	Firebase SMS MFA is implemented and recommended for all users at first login.
PRIVILEGE LEVELS	We support role-based access control: Admin (manages users) and User (standard access).
RESOURCE ACCESS	The platform only requires access to your resources if SharePoint integration is configured, which uses a secure, least-privilege service account (Azure App Registration and MSI Graph API with Sites.Selected).

Data Retention, Auditing & Vendor Assurance

FEATURE	BIDLOGIQ Implementation
TENDER DATA RETENTION	Closed RFP files are automatically and permanently deleted **30 days** after the tender's deadline has passed.
ACCOUNT DATA RETENTION	Basic account information and client metadata is retained for a minimum of **7 years** for legal and business record-keeping.
USER AUDITING	Admins can track timestamped user logins, administrative actions, and basic user activity within the admin panel.
FORMAL CERTIFICATIONS	We are not yet tested for ISO 27001 or SOC 2 certified but are **actively working towards formal certification**.
INCIDENT RESPONSE	We have a clear, severity-based incident response process. A lead developer is on-call to handle critical service issues **within 8 hours of notice**.
PAST DATA BREACHES	We have had **no data breaches**

Note: If using your own SharePoint tenant some features and data retention policies may not apply.