



Data Security & Privacy Policy

How Own Your Numbers protects your financial data

Version: 1.0

Last Updated: 18 November 2025

Effective Date: 18 November 2025

1. INTRODUCTION & SCOPE

1.1 Purpose

This Data Security & Privacy Policy explains how Own Your Numbers ("OYN", "we", "us") collects, processes, stores, and protects your financial data when you use our cash flow analysis service.

1.2 Who This Applies To

This policy applies to all users of the Own Your Numbers platform in production environments, including:

- Business owners and financial directors using our service
- Authorized team members with access to company financial data
- Any third-party service providers processing data on our behalf

1.3 Our Commitment

We are committed to protecting your financial data with enterprise-grade security measures. Your trust is paramount, and we design every aspect of our service with data minimization, transparency, and security at the core.

2. DATA COLLECTION & PROCESSING

2.1 What Data We Collect

When you use Own Your Numbers to generate a cash flow analysis, we process:

- **Financial Data:** Excel files containing trial balances, aged receivables, aged payables, and general ledger information
- **Company Information:** Company name, financial period dates, account classifications
- **Account Information:** Email address, authentication tokens, user preferences
- **Technical Data:** Session identifiers, processing logs, system performance metrics

2.2 What Data We DO NOT Collect

We do not collect or store:

- Payment card information (we do not process payments)
- Personal financial information of your customers or employees
- Social security numbers, tax identification numbers, or similar identifiers
- Bank account credentials or login information, including passwords

2.3 How We Process Your Data

Step 1: Upload & Validation (0-1 minute)

- Your Excel files are uploaded securely via HTTPS/TLS encryption
- Files are validated for format (.xlsx, .xls)
- Files are temporarily stored in secure, isolated storage during processing

Step 2: Data Extraction (1-2 minutes)

- Our system extracts structured financial data from your Excel files
- Key metrics are calculated: cash position, working capital, burn rate, runway
- Monthly snapshots are created for trend analysis
- **Original Excel files are NEVER permanently stored**

Step 3: AI Analysis (Optional, 30-60 seconds)

- A structured financial summary (NOT your raw Excel files) is sent to secure, private Enterprise Google Vertex AI
- The AI generates insights, identifies risks, and recommends priorities
- AI responses are structured and validated before being included in your report

Step 4: Report Generation (30 seconds)

- A PDF report is generated with your financial analysis
- The report is made available for immediate download
- **PDFs are deleted immediately after download**

Step 5: Cleanup (Immediate)

- Temporary Excel files are deleted from our systems
- Processing completes within 2-5 minutes from upload to download

3. DATA RETENTION POLICY

We retain data only as long as necessary to provide our service and comply with legal obligations.

Data Type	Retention Period	Purpose	Storage Location
Original Excel Files	0 hours (temporary only)	Processing only	Temporary system storage, deleted immediately after processing
PDF Reports	0 hours (transient)	Immediate download	Deleted immediately after download completes
Financial Analyses	24 hours maximum	Quality assurance, troubleshooting	Encrypted cloud storage (GCP UK)
Processing Logs	30 days maximum	System diagnostics, error tracking	Encrypted cloud storage (GCP UK)
Account Information	Until account deletion	Authentication, user preferences	Encrypted database (GCP UK)

Automated Deletion:

- Our retention enforcement system runs hourly to automatically delete expired data
- You can request immediate deletion of your data at any time by contacting support@ownyournumbers.app
- Upon account deletion, all associated data is permanently removed within 24 hours

What Our Logs Contain:

- Processing logs contain high-level information only: session IDs, file counts, processing timings, error codes
- **Logs DO NOT contain:** Raw financial values, account balances, transaction details, or personal identifiers

4. INFRASTRUCTURE & HOSTING

4.1 Cloud Infrastructure

Own Your Numbers production environments run on **Google Cloud Platform (GCP)** in the **United Kingdom region**.

All customer data is hosted exclusively within the UK, ensuring compliance with UK GDPR and data residency requirements.

4.2 Security Measures

Encryption in Transit:

- All data transmitted to and from Own Your Numbers is encrypted using HTTPS/TLS 1.2+ protocols
- API communications use secure bearer token authentication
- Email communications use STARTTLS encryption via Mailgun EU servers

Encryption at Rest:

- All data stored on Google Cloud Platform is encrypted at rest using AES-256 encryption
- Database credentials and API keys are encrypted and managed via Infisical (EU region)
- JWT tokens use HMAC-SHA256 signing with strong, randomly generated secrets

Access Controls:

- Passwordless authentication via magic links (single-use, time-limited tokens)
- Role-based access control (RBAC) for administrative functions

5. ARTIFICIAL INTELLIGENCE (AI) PROCESSING

5.1 AI Provider

Own Your Numbers uses **Google Vertex AI Enterprise (Gemini)** to generate financial insights and risk assessments.

5.2 What Data Is Sent to AI

We send **structured financial summaries only** to Vertex AI, including:

- Aggregated balance sheet data (total assets, liabilities, equity)
- Cash flow metrics (bank balance, net cash, burn rate)
- Working capital trends (receivables aging, payables aging)
- Monthly financial snapshots for trend analysis

What Is NOT Sent to AI:

- Your original Excel files
- Individual transaction details
- Customer or vendor names
- Employee information
- Raw accounting entries

5.3 AI Data Protection Guarantees

Google Vertex AI Enterprise provides the following guarantees:

Zero Data Retention: Your data is NOT used to train or improve Google's AI models

No Model Fine-Tuning: Your financial data is never used to fine-tune Gemini or other Google models

Short-Lived Caching: Data may be cached in memory for up to 24 hours for latency optimization only

Enterprise-Grade Security: Vertex AI complies with ISO 27001, SOC 2 Type II, and UK GDPR

For full details, see: [Google Vertex AI Zero Data Retention](#)

6. COMPLIANCE & CERTIFICATIONS

Own Your Numbers leverages Google Cloud Platform's comprehensive compliance certifications:

- **ISO 27001** — International standard for information security management systems
- **ISO 27017** — Cloud-specific security controls and implementation guidance
- **ISO 27018** — Protection of personally identifiable information (PII) in public clouds
- **SOC 2 Type II** — Independent audit of security, availability, and confidentiality controls
- **UK GDPR** — United Kingdom General Data Protection Regulation compliance

These certifications are maintained by Google Cloud Platform. For details, see: [GCP Compliance & Certifications](#)

Our GDPR Commitments:

- **Right to Access:** Request a copy of your data at any time
- **Right to Rectification:** Correct inaccurate data in your account
- **Right to Erasure:** Request deletion of your data (fulfilled within 24 hours)
- **Right to Data Portability:** Export your financial analyses in standard formats

7. AUTHENTICATION & ACCOUNT SECURITY

7.1 Passwordless Authentication

Own Your Numbers uses **magic link authentication** to eliminate password-related security risks:

1. Enter your email address
2. Receive a single-use magic link via email (expires in 15 minutes)
3. Click the link to authenticate securely
4. Session token issued with 1-hour expiry

8. THIRD-PARTY SERVICE PROVIDERS

We use the following third-party services to operate Own Your Numbers:

Service Provider	Purpose	Data Shared	Location	Compliance
Google Cloud Platform	Hosting, compute, storage	All service data	UK (europe-west2)	ISO 27001, SOC 2, UK GDPR
Google Vertex AI	Enterprise AI-powered analysis	Structured financial summaries	EU	Vertex AI zero data retention
Mailgun	Transactional emails	Email addresses, magic links	EU	SOC 2 Type II, GDPR
Infisical	Secrets management	API keys, credentials (encrypted)	EU	SOC 2 Type II

All third-party providers are carefully vetted for security, compliance, and data protection standards.

9. DATA BREACH NOTIFICATION

In the unlikely event of a data breach affecting your information:

1. **Detection:** Our monitoring systems detect unauthorized access or anomalies
2. **Containment:** Immediate action to contain and remediate the breach
3. **Assessment:** Determine scope, affected users, and data types compromised
4. **Notification:** Affected users notified within 72 hours via email
5. **Regulatory Reporting:** UK Information Commissioner's Office (ICO) notified as required by UK GDPR
6. **Remediation:** Root cause analysis and implementation of additional safeguards

Contact for Security Concerns:

Email: support@ownyournumbers.app

Response time: Within 24 hours for security-related inquiries

10. YOUR RIGHTS & CHOICES

10.1 Access Your Data

You can access your financial analyses and account information at any time through your dashboard at ownyournumbers.app.

10.2 Delete Your Data

To request deletion of your data:

1. Contact support@ownyournumbers.app with your account email
2. We will confirm your identity and process your request

11. UPDATES TO THIS POLICY

We may update this Data Security & Privacy Policy from time to time to reflect:

- Changes to our data processing practices
- New regulatory requirements
- Enhanced security measures
- User feedback and requests

Updated policy will be posted at ownyournumbers.app/ui/security. Continued use of the service constitutes acceptance of the updated policy.

Version History:

- Version 1.0: 18 November 2025 — Initial publication

12. CONTACT US

For questions, concerns, or requests regarding this policy:

Support: support@ownyournumbers.app

APPENDIX A: GLOSSARY

Data Controller: The entity that determines the purposes and means of processing personal data (Own Your Numbers)

Data Processor: A third-party service that processes data on behalf of the Data Controller (e.g., Google Cloud Platform, Vertex AI)

Data Subject: An individual whose personal data is processed (you, the user)

Encryption at Rest: Data is encrypted when stored on disk or in databases

Encryption in Transit: Data is encrypted when transmitted over networks (HTTPS/TLS)

Magic Link: A single-use authentication URL sent via email that expires after 15 minutes

Personal Data: Any information relating to an identified or identifiable individual

Retention Period: The length of time data is stored before automatic deletion

Session Token: A temporary credential that authenticates your session (expires after 1 hour)

Structured Financial Summary: Aggregated financial metrics sent to AI (not raw Excel files)

— End of Policy —