



Data Protection Executive Summary

Data Handling & Privacy Practices — Version 1.0 · 2026

Document	Data Protection Executive Summary
Audience	Clients, prospects and partners
Owner	Chief Operations Officer / ISO
Review frequency	At least annually
Contact	security@wiseathena.com

1. Overview

WiseAthena is a B2B technology company providing data analytics and processing services to business clients. This document summarises how WiseAthena handles data — both the client data processed as part of service delivery, and the limited personal data the organisation holds about its own workforce.

Data protection is an integral part of WiseAthena's Information Security programme, which is aligned to the SOC 2 Security Trust Services Criteria.

2. Types of Data We Handle

CATEGORY	DESCRIPTION	HOW IT IS TREATED
Client business data	Data provided by B2B clients for analytics and processing services	Treated as commercial information. Processed solely to deliver contracted services. Subject to strict confidentiality controls.
Commercial information	Prospect and client contact details held for business relationship management	Managed as commercial data in our CRM. Not used for purposes other than business relationship management.
Workforce personal data	Personal data of employees and contractors (HR, payroll, access management)	Processed for employment and contractor management purposes only, under applicable labour and data protection law.

3. Core Data Protection Principles

WiseAthena applies the following principles to all data it holds and processes:

- **Purpose limitation** — data is collected and used only for the specific, documented purpose for which it was received
- **Data minimisation** — we collect only the data necessary to deliver our services
- **Confidentiality** — access to data is restricted to authorised personnel on a need-to-know basis
- **Integrity** — controls are in place to prevent unauthorised modification or destruction of data
- **Security** — technical and organisational measures protect data against unauthorised access, loss or disclosure
- **Retention** — data is retained only for as long as necessary for its purpose or as required by applicable law

4. Security Controls Protecting Data

Data is protected by the controls defined in WiseAthena's Information Security programme, which include:

CONTROL	DESCRIPTION
Access control	Access to data assets is granted on a least-privilege basis and reviewed periodically
Multi-factor authentication	MFA is required for all remote access to systems holding sensitive data
Encryption	Data is protected with appropriate encryption in transit and at rest
Monitoring & logging	Security events are monitored and anomalous activity is investigated
Vendor oversight	Third-party providers that process data on our behalf are subject to formal security assessment and ongoing review
Incident response	A documented incident response process governs the detection, containment and notification of data security events

5. Regulatory Compliance

WiseAthena operates as a B2B data processor and analytics provider. Our data protection practices are designed to be compatible with applicable regulations in the jurisdictions in which we operate. Relevant considerations include:

- Data processing agreements (DPAs) are available for clients who require them
- In the event of a security incident affecting personal data, the organisation has defined procedures for timely notification to relevant regulatory authorities and affected parties
- Workforce personal data is processed in compliance with applicable employment and data protection law

Clients who operate in regulated sectors (financial services, healthcare, etc.) and have sector-specific compliance requirements are encouraged to contact us to discuss their needs.

6. Data Processed on Behalf of Clients

When WiseAthena processes data on behalf of a client as part of service delivery, the following principles apply:

- Data is processed solely according to the client's instructions and the terms of the agreed contract
- Client data is not used for any purpose other than the delivery of the contracted service
- Access to client data is restricted to personnel who require it to perform their role
- Client data is not shared with third parties except where required for service delivery, and subject to appropriate contractual protections
- Upon contract termination, data retention and deletion are handled according to the terms agreed in the contract

7. Contact

For questions about WiseAthena's data protection practices, or to request a Data Processing Agreement, please contact:

Data protection enquiries

security@wiseathena.com
