TrackView Privacy Statement and Liability Waiver

For

Azure Managed Application

27th November 2025

Version 1

Table of Contents

1. Privacy Statement

This Privacy Statement describes how Techno Management (“we”, “us”, “our”) collects, uses, stores, and protects information processed by the TrackView application (“the Application”). The Application is delivered through the Microsoft Azure Marketplace as an Azure Managed Application and operates within the customer’s Azure environment under their control.

By deploying or using the Application, you (“Customer”, “you”) consent to the data practices described in this Privacy Statement.

1.1 Scope of the Application

The Application is installed within your Azure subscription. All operational data processed by the Application remains inside your environment unless explicitly configured by you to be transmitted externally.
This Privacy Statement applies specifically to:

1. The Application’s behavior and data handling
2. Any diagnostic or operational data optionally sent to us
3. Support interactions initiated by the Customer

1.2 Data Collected

1.2.1 Data Stored in the Customer’s Environment

The Application may process the following types of data within your Azure subscription:

1. Configuration data required for deployment
2. Logs generated by the Application
3. Operational metadata (e.g., resource names, environment parameters)
4. Any customer data explicitly connected to the Application’s functionality

All such data remains fully under Customer ownership and control.

1.2.2 Data Transmitted to Techno Management

By default, the Application does not transmit any data to us.
Only the following data may be collected, and only if the Customer explicitly opts in:

1. Error logs or diagnostic reports voluntarily submitted
2. Support-related information shared during troubleshooting

3. Telemetry (if enabled), such as feature usage statistics or performance data

1.3 Purpose of Data Use

Data collected may be used for:

1. Delivering technical support
2. Troubleshooting issues and improving reliability
3. Enhancing Application performance and functionality
4. Identifying usage patterns (if telemetry is enabled)

We do NOT:

1. Access your environment without authorization
2. Sell personal or operational data
3. Use Customer data for marketing

1.4 Storage and Security

For any Customer data transmitted to us:

1. It is stored in secure, access-controlled systems
2. Access is restricted to authorized personnel
3. Industry-standard security controls are applied

Data stored within your own Azure subscription is governed by your organization's security and compliance standards.

1.5 Data Retention

We retain collected data only for as long as necessary to:

1. Provide support
2. Resolve issues
3. Comply with legal or operational requirements

Support-related data may be deleted upon Customer request.

1.6 Customer Control and Access

You maintain full control over:

1. All data residing in your Azure environment
2. Telemetry or diagnostic data-sharing settings
3. Whether and when to provide logs or troubleshooting information

1.7 Third-Party Services

The Application may rely on Azure-native services (e.g., Storage Accounts, Key Vault, Application Insights). Any data stored in these services remains governed by:

1. Your Azure subscription
2. Microsoft's privacy and compliance policies

We do not share Customer data with third parties except when required by law.

1.8 Compliance

Our data handling practices are designed to align with:

1. GDPR
2. Microsoft Commercial Marketplace requirements
3. Industry best practices for cloud privacy

If required, we can provide additional compliance documents or DPAs upon request.

1.9 Contact Information

For questions or privacy requests, contact us at:

Techno Management
contact@techno-management.com
https://techno-management.com/track-view

1.10 Updates to This Privacy Statement

We may update this Privacy Statement periodically. Updated versions will be published in the Azure Marketplace listing and on our website. Continued use of the Application constitutes acceptance of the updated statment.

2. Liability Waiver

2.1 Purpose of the Liability Waiver

This Liability Waiver Policy (“Policy”) defines the responsibilities, limitations, and expectations between Techno Management (“Vendor”) and the Customer when using the TrackView application hosted on Microsoft Azure Marketplace. This Policy protects the Vendor from liabilities arising from circumstances beyond reasonable control and clarifies the Customer’s obligations to follow recommended best practices.

2.2 Scope

This Policy applies to all users, organizations, and entities accessing, deploying, or managing the TrackView Azure Managed Application.

2.3 Customer Responsibilities

The Customer acknowledges and agrees they are responsible for:
- Managing their Azure subscription, costs, configurations, networking, and security.
- Maintaining proper Azure resource configurations.
- Performing data backups and implementing retention policies.
- Following Vendor-recommended operational and security best practices.

2.4 Vendor Responsibilities

The Vendor is responsible for:
- Delivering the application package through the Azure Marketplace.
- Ensuring deployment succeeds when Azure resources are correctly provisioned.
- Providing documentation and best-practice recommendations.
- Support as per published support guidelines.

2.5 Waiver of Liability

2.5.1 Data Loss

Vendor is not responsible for:
- Loss, corruption, or alteration of Customer data.

- Data deletion caused by Customer actions or integrations.
- Issues caused by insufficient backup or retention settings.

2.5.2 System Unavailability

Vendor is not liable for:
- Azure service outages.
- Customer misconfigurations.
- Third-party system dependencies or failures.
- Force majeure events.

2.5.3 Security Breaches

Vendor is not responsible for:
- Breaches caused by Customer-managed Azure settings.
- Weak credentials or compromised identities.
- Malware or malicious scripts introduced through Customer systems.

2.5.4 Other Situations Beyond Vendor Control

Including but not limited to:
- Azure cost overruns.
- Performance issues due to insufficient resource sizing.
- API throttling by Azure or third parties.

2.6 Customer Acknowledgment of Best Practices

Customer agrees to follow best practices including redundancy, RBAC least privilege, backup configuration, and use of Azure Defender/Security Center.

2.7 Limitation of Liability

Vendor liability is limited to the amount paid for the application (if any). Vendor is not liable for indirect or consequential damages.

2.8 Support Boundaries

Vendor support includes application-level issues only and excludes Azure infrastructure debugging, data restoration, and customer-caused security problems.

2.9 Acceptance

By deploying or using the application, the Customer acknowledges and accepts this, Policy.

2.10 Amendments

Vendor may update this Policy at any time. Continued use constitutes acceptance.

2.11 Contact

Techno Management
contact@techno-management.com
https://techno-management.com/track-view