



Service Level Agreement

REGULAR · VERSION 2.0

Effective 26 September 2026

1. Agreement overview

This Service Level Agreement (the "SLA") is made between DataTako B.V., Antareslaan 65, 2132 JE Hoofddorp, the Netherlands, Chamber of Commerce (KvK) number 42129309 (the "Service Provider"), and the customer holding a valid DataTako licence (the "Customer"), for the provision of the services necessary to support and maintain DataTako (the "Service").

This SLA remains in effect until replaced by a revision approved by both Parties. It defines the terms and parameters of the services covered and does not override any existing process or procedure unless expressly stated here.

This SLA forms part of the agreement between the Parties together with the DataTako General Terms and Conditions and the DataTako Data Processing Agreement. Where this SLA and the Data Processing Agreement conflict in respect of the processing of personal data, the Data Processing Agreement prevails.

2. Goals and objectives

The purpose of this SLA is to establish the commitments needed to deliver consistent support and service to the Customer, and to create a shared understanding between the Parties of what is and is not covered. Its objectives are to:

- define service ownership, accountability, roles and responsibilities;
- provide a clear, concise and measurable description of the services offered;
- align the Customer's expectations with the support and service actually provided.

3. Service levels

Availability guarantee	99.5%, measured over a calendar month, excluding maintenance windows and any downtime caused by Microsoft services, including Power BI, Microsoft Fabric and the Azure platform.
Maintenance windows	Approximately 6 hours per month. Where planned downtime is expected to exceed 10 minutes, the Customer is notified in advance.
Unplanned downtime	Where unplanned downtime exceeds 10 minutes, the Customer is notified without undue delay and kept informed until the Service is restored.
Support window	Monday to Friday, 09:00 to 17:00 (CET/CEST). Support outside these hours is not guaranteed and may be subject to additional lead time.

4. Response and resolution times

The guaranteed response and resolution times depend on the severity of the disruption:

Severity	Definition	Response	Resolution
Very High	Complete outage. All users are affected; the component or service is entirely unreachable.	4 hours	8 hours
High	Significant disruption. A large number of users and critical business processes are affected.	8 hours	16 hours
Medium	Limited disruption. A number of users and functionalities are affected.	24 hours	72 hours
Low	An individual user or a single functionality is affected.	32 hours	72 hours

These times are measured in business hours within the support window (Monday to Friday, 09:00 to 17:00 CET/CEST), unless otherwise agreed between the Parties in writing.

These are support targets for responding to and resolving a reported disruption. They are distinct from the recovery objectives in section 5, which apply to the restoration of the Service and of the data after a serious disruption and are measured in elapsed clock

hours. Where the two differ, the recovery objectives govern restoration and the times above govern the handling of the support request.

5. Continuity, backup and recovery

DataTako maintains the following objectives for the systems and data it manages, being platform accounts, authorisations, and platform and report configuration:

Objective	Commitment
Recovery Time Objective (RTO)	24 hours. Essential platform functionality is restored within 24 elapsed clock hours from the start of a service disruption.
Recovery Point Objective (RPO)	24 hours. The maximum intended loss of recent changes to platform data is 24 hours.
Backup frequency and retention	Daily automated backups, retained for 30 days, stored encrypted in a secure remote location sufficiently separated from the primary site of processing.
Testing	Backup restoration is tested at least annually, and the Business Continuity and Disaster Recovery Plan is tested at least annually.

Power BI and Microsoft Fabric semantic models and the source data hosted in the Customer's own Microsoft environment are subject to the Customer's own backup and recovery arrangements.

6. Third parties

DataTako cannot guarantee the times set out in section 4 where resolution depends on infrastructure or follow-up by a third party, including Microsoft and the hosting provider. In such cases DataTako will inform the Customer of the dependency, pursue the third party actively, and keep the Customer informed of progress.

7. Security commitments

In providing the Service, DataTako commits to the following measures to protect the security and confidentiality of Customer data:

- Data minimisation by design. DataTako stores report metadata, user accounts and access permissions only. Report content, visuals, query results and source data remain in the Customer's own Microsoft environment and are not stored, cached or retained by DataTako.
- Access to the systems supporting the Service is restricted to authorised DataTako personnel on a least-privilege basis under a documented role-access matrix. Every member of personnel has a unique named account, multi-factor authentication is required on the accounts used to administer the Service, and administrative access to production is possible only over encrypted protocols from whitelisted, labelled IP addresses.
- Customer data is encrypted in transit over public networks using TLS 1.2 or higher, and stored platform data and backups are encrypted at rest.
- Logical separation between customers is enforced at both the application and the database layer, and is re-verified after any restore before customer access is restored.
- Changes affecting the Service, including security configuration, are recorded as change requests and reviewed and approved by a second person before release. No person approves or releases their own change.
- The production environment is configured to a documented hardening baseline based on the applicable CIS Benchmarks and the Microsoft Security Baseline, and is scanned for vulnerabilities at least quarterly and after significant changes.
- Personal data is processed in accordance with the DataTako Data Processing Agreement, which is the processing agreement between the Parties for the purposes of Article 28 GDPR. Personal data breaches are notified to the Customer in accordance with that agreement.

8. Assurance

DataTako maintains a documented information security programme, including an Information Security Policy, a System Hardening Standard and a Business Continuity and Disaster Recovery Plan, which is approved by the Risk Committee and reviewed at least annually.

DataTako is currently completing a SOC 2 Type 1 audit performed by an independent auditor. No SOC 2 report is available yet. Once the report has been issued, it will be made available to Customers on request under a non-disclosure agreement, and DataTako intends to follow it with a SOC 2 Type 2 examination covering an observation period. Pending issuance, DataTako can provide a letter of engagement from its auditor confirming that the audit is under way and its scope.

DataTako has not yet had an external penetration test performed. One is foreseen during the SOC 2 Type 2 observation period.

Security documentation, including the Information Security Policy and the current sub-processor list, is available to Customers on request under a non-disclosure agreement.

9. Document control

Version	Date	Change
1.x	2026	Previous editions, issued without a version number.
2.0	26-09-2026	Assurance section rewritten to state the actual SOC 2 status in place of an annual independent examination that had not taken place; reference to the NLdigital Data Pro Statement replaced by the DataTako Data Processing Agreement; recovery objectives, backup frequency and retention added; the relationship between support times in business hours and recovery objectives in clock hours clarified; multi-factor authentication commitment scoped to the accounts used to administer the Service; encryption at rest, hardening baseline and vulnerability scanning added; legal entity, address and Chamber of Commerce number added; document control and versioning introduced.