DataTako
Information Security Policy

Technical and organisational measures protecting customer data on the DataTako platform.

Document owner	DataTako B.V.
Version	2.3
Effective date	5 May 2026
Next review	5 May 2027 (annual)
Contact	security@datatako.com

1. About this document

This document describes the technical and organisational measures (TOMs) that DataTako B.V. ("DataTako") applies to protect the confidentiality, integrity and availability of customer data processed through the DataTako platform.

It is intended to support customer vendor-security reviews and to serve as the security annex to our Data Processing Agreement (GDPR Article 32). Additional detail is available under NDA on request.

Scope. This policy covers the DataTako SaaS platform, the supporting cloud infrastructure operated by DataTako, and all DataTako personnel and contractors with access to production systems or customer data. It does not cover customers' own environments, end-user devices, or any third-party systems with which customers choose to integrate.

2. Assurance and compliance position

DataTako's information security programme is designed in alignment with the controls of **ISO/IEC 27001:2022** (Annex A) and the security-of-processing requirements of **GDPR Article 32**.

Independent attestation roadmap. DataTako has engaged an independent auditor and is actively pursuing SOC 2 attestation:

- **SOC 2 Type I** — audit contracted and scheduled to complete in **Q4 2026** (before the end of 2026).
- **SOC 2 Type II** — scheduled to follow the Type I report, with completion targeted by the **end of July 2027**.

Until those reports are issued, DataTako is **not** yet independently certified against SOC 2, and is not certified against ISO/IEC 27001. We are transparent about that position.

Inherited assurance from key partners. DataTako delivers the service in conjunction with parties that already hold recognised independent certifications:

- **Microsoft Azure** — provides the primary hosting platform and is independently certified against ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3, C5, and other recognised frameworks.
- **Hetzner Online (Germany)** — provides supporting stateless compute capacity and is independently certified against **ISO/IEC 27001**.
- **DataTako's principal development partner** — holds **ISO/IEC 27001** certification covering its software-engineering activities, which provides additional assurance over the development process for the platform.

Where customer data is processed by sub-processors, those parties are likewise selected on the basis of recognised certifications and contractual safeguards.

We will complete customer-supplied security questionnaires on request and can discuss the certification roadmap and the underlying engagement directly.

3. Governance and risk management

- A named member of management is accountable for information security and for this policy.
- Security risks are identified, assessed and reviewed on a recurring basis. Material risks are documented together with the controls that mitigate them.
- This policy is reviewed at least annually, and whenever there is a material change to the platform, the threat landscape, or applicable law.
- Changes to the policy are approved by management before they take effect.

4. People security

- All personnel and contractors with access to production systems or customer data are bound by written confidentiality obligations.
- Access is granted on the basis of role and the principle of least privilege, and is provisioned, modified and revoked through a documented joiner / mover / leaver process.
- All personnel receive security awareness guidance at onboarding and on a recurring basis thereafter, covering at minimum: handling of customer data, recognition of social-engineering attempts, secure use of credentials and devices, and incident reporting.
- Workstations used for production access are required to have full-disk encryption, automatic screen locking, and current operating-system and security patches.

5. Access control and authentication

5.1 Customer-facing access

- The platform supports authentication via username/password, **single sign-on (SAML 2.0 and OpenID Connect)** with major identity providers, and **multi-factor authentication** for end-users.
- Password handling follows current good practice: minimum length and complexity requirements are enforced, and stored credentials are protected with a salted, computationally hard one-way function.
- Access within a customer tenant is governed by **role-based access control**, administered by the customer's own administrators.
- Sessions are time-bounded; long-lived session credentials can be revoked centrally and are invalidated on sign-out and on administrator request.
- Programmatic access uses scoped, cryptographically signed API credentials. Credential secrets are stored in hashed form; the original value is shown to the user once at creation and cannot be retrieved later. Programmatic interfaces are protected by per-credential rate limits to mitigate brute-force and abuse.
- Cross-origin access to platform APIs is restricted to known DataTako application origins.

5.2 Internal access to production

- Access to production infrastructure, data and deployment systems is restricted to a small number of authorised engineers on a need-to-know basis.
- All such access requires individually-attributable accounts protected by **multi-factor authentication**.
- Access is reviewed periodically and on every staffing change, and is revoked promptly when no longer required.
- Direct access to customer data and reports by DataTako support staff is **not available by default**. Where access is required for support or incident response, it must be explicitly granted by the

customer by inviting the support team into their organisation. All such access is controlled, logged, and individually attributable.

6. Cryptography and data protection

- **Data in transit.** All communication between customers and the platform, and between the platform's components and managed cloud services, is protected with **TLS 1.2 or higher** using current cipher suites. Plain HTTP is redirected to HTTPS, and HTTP Strict Transport Security (HSTS) is enforced.
- **Data at rest.** Customer data and backups are encrypted at rest using **AES-256** through the cloud platform's managed encryption services.
- **Key management.** Cryptographic keys are managed by the cloud platform's managed key service, with access restricted to authorised production identities and with rotation in line with platform defaults.
- **Secrets management.** Application secrets (database credentials, third-party API keys, signing keys) are held in a managed secrets store and made available to the application at runtime through cloud-managed identities. Secrets are not stored in source code or in configuration files held in source control. Access to the secrets store is logged.

7. Application and product security

- Software is developed under a defined secure-development process. Every change to production code is reviewed and approved by **at least one engineer other than the author** ("four-eyes principle") before it can be merged.
- Reviewers are expected to consider security implications — including input handling, authorisation, tenant scoping, and handling of secrets — as part of every review.
- The build and release pipeline is automated; production deployments are produced from reviewed source in a controlled environment, not from individual workstations.
- Application input is validated server-side before it is acted on. Database access uses parameterised queries to prevent injection attacks.
- Authentication, session management and access-control logic is implemented using established platform components rather than bespoke cryptography.

8. Vulnerability and patch management

- The platform runs on actively-supported versions of its runtime, database and operating-system components. Patching of the underlying managed services is performed by the cloud platform.
- Application dependencies are scanned **periodically and on a recurring basis** for known vulnerabilities. The application's own source code is subject to **automated security analysis**.
- Identified vulnerabilities are triaged on the basis of severity and exploitability. Critical and high-severity issues affecting production are remediated as a matter of priority; lower-severity issues are scheduled into the regular development cycle.
- Vulnerability reports from external parties are welcomed at **security@datatako.com** and handled under our coordinated-disclosure approach.

9. Operations, logging and monitoring

- Application and infrastructure events are written to centralised, structured logs.
- Application errors and anomalies are surfaced in real time to the engineering team for investigation.
- Material business records carry an immutable audit trail of who created, modified or deleted them, and when. This audit trail is generated by the platform itself and cannot be bypassed by ordinary application code.
- Security-relevant events within a customer tenant are visible to that customer's administrators.
- Capacity, availability and error-rate indicators are monitored continuously, with alerting on defined thresholds.

10. Infrastructure and tenant isolation

- The platform is hosted across **Microsoft Azure** and **Hetzner Online**, both in EU regions (Microsoft Azure West Europe by default; Hetzner Online in Germany). Stateful customer data — including the application database — is held on Microsoft Azure. Hetzner Online provides stateless supporting compute for the rendering service and the public API gateway; **no customer data is persisted at rest on Hetzner**, and transient processing artefacts are discarded after rendering.
- The platform is **multi-tenant**. Each customer's data is logically segregated and is accessed through a tenant-scoping enforcement layer that automatically restricts every data access to the calling tenant's records.
- Production, staging and development environments are segregated. Production data is not used in non-production environments.
- Network access to backing data stores is restricted to the application's own production identities; data stores are not directly reachable from the public internet.

11. Sub-processors and supply chain

DataTako engages a small set of carefully selected sub-processors to deliver the service. The current sub-processor list, including the categories of data processed and the location of processing, is maintained as a separate document and is available on request.
Sub-processors are selected on the basis of:

- Recognised independent assurance (ISO/IEC 27001, SOC 2 Type II, or equivalent), or a documented assessment where such certification is not available.
- A written contract incorporating the GDPR Article 28 processor obligations, including international-transfer safeguards (typically the EU Standard Contractual Clauses) where applicable.
- Periodic re-review.

Customers are notified of material changes to the sub-processor list in line with the relevant Data Processing Agreement.

12. Incident response

- DataTako maintains a defined incident-response approach covering detection, triage, containment, eradication, recovery and post-incident review.
- Where a confirmed **personal-data breach** affecting customer data occurs, DataTako will notify affected customers without undue delay and in any case within the timelines and content requirements of GDPR Article 33–34 and the relevant Data Processing Agreement, so that customers can in turn meet their own notification obligations.

- Each significant incident is followed by a documented root-cause analysis, with corrective actions tracked through to completion.

13. Business continuity, backup and recovery

- Customer data held in the production database is protected by **automated, encrypted backups** managed by the cloud platform, in line with the published retention defaults of the chosen service tier.
- The platform is deployed on cloud services that provide redundancy at the infrastructure layer.
- DataTako periodically verifies that the application can be redeployed from source control to a clean environment.
- Formal recovery-time and recovery-point objectives (RTO / RPO) are not currently published in this document; they can be discussed in the context of a specific contract.

14. Privacy, data retention and data-subject rights

- DataTako processes personal data as a **processor** on behalf of its customers, under a written **Data Processing Agreement** that incorporates GDPR Article 28 requirements.
- Customer data is processed within the European Union by default. Where a sub-processor processes data outside the EU, transfers are covered by the **EU Standard Contractual Clauses** of the relevant provider, supplemented as required by case law.
- Customers can export their tenant data through the platform.
- On confirmed customer request, or upon termination of the contract, customer data is removed from production systems within a reasonable timeframe. Residual copies in encrypted backups age out as those backups expire.
- DataTako will assist customers in responding to data-subject requests in line with the Data Processing Agreement.

15. Customer responsibilities

Security of the overall solution is a shared responsibility. Customers are expected to:

- Manage their own users, roles, and the lifecycle of those accounts within their tenant.
- Enforce multi-factor authentication for administrative users and other sensitive roles.
- Protect any API credentials issued to them and rotate them on suspected compromise.
- Only upload personal or other regulated data to the platform where they have a valid lawful basis, and in line with the agreed scope of processing.
- Notify DataTako promptly at **security@datatako.com** on becoming aware of any security issue affecting their tenant.

16. Contact

For security questions, vulnerability reports, or to request the latest version of this document, the sub-processor list, or supporting evidence under NDA:

security@datatako.com

We aim to acknowledge security-related correspondence within two business days.