DataTako privacy statement

Effective date: 01-02-2026
Last updated: 01-02-2026
Version: 2.0

1. Introduction

This Privacy Statement (the "Statement") describes how DataTako B.V. ("DataTako", "we", "us", or "our") collects, uses, discloses, and otherwise processes personal data in connection with the DataTako software-as-a-service platform (the "Service"), the website at www.datatako.com, and all related applications, APIs, and customer-facing interfaces (together, the "Platform").

This Statement is designed to comply with Regulation (EU) 2016/679 (the General Data Protection Regulation, "GDPR"), the EU ePrivacy Directive (2002/58/EC) as transposed in the relevant Member States, and applicable national data protection legislation. Where DataTako processes personal data on behalf of a customer (as further described in Section 4), this Statement is supplemented by the Data Processing Agreement ("DPA") concluded between DataTako and that customer.

By using the Platform, data subjects acknowledge that their personal data may be processed as described in this Statement. This Statement does not, by itself, constitute a contract between DataTako and any data subject and does not waive rights granted under the GDPR.

2. Who we are

DataTako is operated by:

Field	Detail
Legal entity	DataTako B.V.
Legal form	Besloten Vennootschap / B.V.
Registered office	Antareslaan 65, 2132JE Hoofddorp
Chamber of Commerce / company number	96958081
VAT number	NL867850292B01
General contact	info@datatako.com
Privacy contact	privacy@datatako.com
Data Protection Officer	Not appointed; a designated privacy contact is reachable at privacy@datatako.com

DataTako is established in the European Union and the Platform is hosted within the European Union (see Section 9).

3. Roles: Controller and Processor

DataTako acts in two distinct capacities under the GDPR, and the legal basis, retention period, and rights-handling procedure depend on which capacity applies to a given processing activity.

3.1 DataTako as Processor

For personal data that is uploaded to, embedded in, or otherwise made available within reports, dashboards, datasets, content items, media items, or other customer-controlled resources on the Platform, the customer (typically the organization that has subscribed to the Service) is the **controller**. DataTako acts as **processor** and processes such data solely on documented instructions from the customer in accordance with the DPA.

This includes, in particular:

- Personal data appearing within Power BI reports, datasets, or visualizations embedded through the Platform;
- Personal data uploaded as media items, files, or content;
- End-user data created or managed by a customer's administrators within their tenant (for example, end-user accounts the customer provisions to access reports).

For these processing activities, the customer determines the purposes and means, the legal basis, the retention period, and is responsible for handling data subject requests in the first instance. DataTako will assist the customer in fulfilling its obligations as required by Article 28 GDPR.

3.2 DataTako as Controller

DataTako acts as **controller** for personal data processed for its own purposes, including:

- Account registration and management of administrative users who sign up for the Service;
- Billing, invoicing, and contract administration;
- Service security, fraud prevention, and abuse detection;
- Service operation, monitoring, error diagnostics, and platform improvement;
- Direct communications with customers (for example, service announcements, security notices, and support);
- Compliance with legal obligations to which DataTako is subject;
- Operation of the public website www.datatako.com.

For these activities, the legal bases set out in Section 6 apply.

4. Personal data we process

The categories of personal data DataTako processes depend on the role described in Section 3 and on the way the Platform is used.

4.1 Account and identity data

Collected directly when a user account is created or invited, or received from an identity provider through single sign-on.

- Full name, first name, last name
- Email address
- Username
- Phone number (where provided)
- Password (stored exclusively as a salted hash; the plaintext password is never stored)
- Two-factor authentication state and authenticator key (where 2FA is enabled)
- Security stamp and password reset codes (operational tokens used for authentication and recovery)
- Preferred user-interface language
- External identity provider identifier (where the user authenticates via Microsoft Entra ID, SAML, or another supported SSO provider)
- Account state metadata: creation time, last modification time, last login time, soft-deletion flag

4.2 Tenant (organization) data

For each customer organization ("tenant"), DataTako stores administrative information including organization name, postal address, city, country code, and primary domain name, together with administrative configuration such as inactivity timeout, IP whitelist settings, and 2FA policy.

4.3 Authentication and session data

- JWT access tokens and refresh tokens issued upon authentication
- Single sign-on profile configuration where the customer has configured SAML 2.0 (identity provider entity ID, sign-on URL, single-logout URL, certificate, metadata URL)
- OAuth client identifiers used for Microsoft Entra ID, Power BI, and Microsoft 365 SMTP integrations

4.4 Technical and usage data

- IP address (collected on each request and used for IP whitelist enforcement, security, and audit purposes; the address is normalized from the connection or, where applicable, from the X-Forwarded-For header)
- HTTP request metadata, user agent, correlation identifier
- Application logs, including the username associated with a request, written to structured server-side logs
- Audit log records of administrative and security-relevant actions, including action name, payload, response status code, response body excerpt, duration, exception details (where applicable), tenant identifier, user identifier, and impersonator identifier (where an authorized administrator acts on behalf of another user)
- Page views, navigation events, click and interaction events, session duration, and traffic source, where the relevant analytics integrations are active and the user has consented to non-essential cookies

4.5 Billing data

Billing identifiers and subscription state are processed by DataTako in connection with the contractual relationship with paying customers:

- Stripe customer identifier, subscription identifier, subscription item identifier, price identifier
- Subscription status, seat count, current period end
- Invoice and payment history references

DataTako does **not** store full payment card numbers or bank account credentials. Payment credentials are entered by the customer directly into Stripe's hosted payment interface and are processed by Stripe, Inc. as an independent controller for payment-card processing (see Section 8).

4.6 Communications data

- Email address, name, and locale used to deliver transactional messages (account activation, password reset, invitations, subscription notifications, smart alerts)
- Where a customer configures a custom SMTP server, the SMTP host, username, password (encrypted), port, and "from" address are stored in order to deliver mail through that server
- Support correspondence and any personal data the user voluntarily includes in such correspondence

4.7 Power BI integration data

To enable embedded Power BI functionality, DataTako stores Microsoft service account credentials configured by the customer (Azure object identifier) and metadata about the workspaces and reports the customer has linked (workspace identifier, workspace name, report identifier, report name, embed configuration, and row-level security flag).

DataTako does **not** ingest, copy, or persist the underlying datasets that customers visualize through Power BI. Report content is rendered on demand by Microsoft's Power BI service; DataTako stores only the metadata necessary to manage and embed reports.

4.8 Customer-controlled data within reports and content

Personal data that customers choose to display in reports, dashboards, media items, or other content items may include any personal data category determined by the customer. This data is processed on the customer's instructions in DataTako's processor capacity (see Section 3.1).

4.9 Data we do not knowingly process

The Platform is intended for business use and is not directed at children. DataTako does not knowingly collect personal data from children under the age of 16. The Platform is not designed to process special categories of personal data (Article 9 GDPR) or data relating to criminal convictions and offences (Article 10 GDPR); customers should not upload such data without first concluding any additional contractual arrangements required by the GDPR and notifying DataTako.

5. Purposes of processing

DataTako processes personal data for the following purposes:

1. **Provision of the Service** — authenticating users; rendering reports; managing tenants, content, and permissions; enforcing access controls; delivering features the customer has subscribed to.

2. **Account administration** — creating, modifying, and deactivating user accounts and tenant configurations; managing invitations; enforcing security policies (2FA, inactivity timeout, IP whitelisting).
3. **Billing and contract management** — issuing invoices, processing subscriptions, calculating seat usage, managing renewals.
4. **Customer support** — responding to support requests and diagnosing reported issues.
5. **Security, fraud prevention, and abuse detection** — monitoring for unauthorized access, brute-force attempts, and abuse; bot detection via reCAPTCHA on public-facing forms; maintaining audit trails.
6. **Service reliability and quality** — collecting application logs, error reports, and performance traces; investigating incidents; restoring service.
7. **Service improvement and product analytics** — analyzing aggregated usage patterns to understand feature adoption and improve the Platform.
8. **Communications** — sending transactional emails, security notices, and (where the recipient has opted in or where permitted under applicable law) service-related announcements.
9. **Legal compliance** — meeting tax, accounting, anti-money-laundering, and other legal obligations; responding to lawful requests from competent authorities.
10. **Defence and enforcement of legal claims** — establishing, exercising, or defending legal claims to which DataTako is a party.

6. Legal bases for processing

DataTako relies on the following legal bases under Article 6(1) GDPR.

Processing activity	Legal basis
Provision of the Service to a customer; account administration; authentication	Article 6(1)(b) — performance of a contract with the customer or pre-contractual steps at the customer's request
Billing, invoicing, subscription management	Article 6(1)(b) — performance of contract; Article 6(1)(c) — compliance with legal obligation (tax, accounting)
Security, fraud prevention, audit logging, abuse detection	Article 6(1)(f) — legitimate interests of DataTako and its customers in maintaining a secure service; Article 6(1)(c) where required by law
Service reliability monitoring, error diagnostics, application logs	Article 6(1)(f) — legitimate interest in operating a reliable service
Product analytics and service improvement (where active)	Article 6(1)(a) — consent (where the analytics rely on non-essential cookies or similar technologies); otherwise Article 6(1)(f)
Direct service communications	Article 6(1)(b) — performance of contract; Article 6(1)(f) — legitimate interest in keeping users informed about the Service they use

Processing activity	Legal basis
Marketing communications to existing customers	Article 6(1)(f), subject to a clear right to object; Article 6(1)(a) where required
Compliance with legal obligations and responses to authorities	Article 6(1)(c)
Establishment, exercise, or defence of legal claims	Article 6(1)(f)
Processing on behalf of a customer (DataTako as processor)	Article 28 GDPR; the legal basis is determined and documented by the customer

A balancing test in respect of each legitimate-interest basis is documented internally and is available on reasoned request.

7. Data retention

DataTako retains personal data only for as long as necessary to fulfil the purposes set out in Section 5 or to comply with legal obligations.

Data category	Retention
User account and tenant data	For the duration of the contract with the customer. Following termination, accounts are flagged as deleted (soft-deleted). Hard deletion of soft-deleted records occurs in line with the schedule set out in the DPA, or upon documented written instruction from the controller, subject to overriding legal retention obligations.
Refresh tokens	Hard-deleted automatically seven (7) days after revocation or expiry.
Audit logs	Retained for 6 months for security and compliance purposes, after which they are deleted or irreversibly anonymized, save where a longer retention period is required by law or to handle an active incident.
Application logs	Retained on a rolling basis as configured in the platform, typically 90 days.
Billing records and invoices	Retained for the period required by applicable tax and accounting law (7 years).

Data category	Retention
Customer-controlled data (DataTako as processor)	Retained for the period determined by the customer in accordance with the DPA. Customers may export and delete such data at any time during the term of the contract, and on termination in accordance with the DPA.
Support correspondence	Retained for 24 months following resolution of the matter.
Marketing contact data	Retained until the data subject objects or withdraws consent, after which the contact is suppressed.

Where personal data is no longer needed and no legal retention obligation applies, DataTako deletes or irreversibly anonymizes the data.

8. Data sharing and subprocessors

DataTako does not sell personal data and does not share personal data with third parties for their own marketing purposes.

DataTako shares personal data with the following categories of recipients:

- **Customers** — administrative users within a customer's tenant may have visibility into other users in the same tenant, as configured by the customer.
- **Subprocessors** — third-party service providers that process personal data on DataTako's behalf under written agreements that comply with Article 28 GDPR.
- **Independent controllers** — for example, payment service providers acting as controllers for payment-card data they process directly.
- **Competent authorities** — where DataTako is required to do so by law, court order, or binding decision of a supervisory authority.
- **Acquirers and successors** — in the event of a merger, acquisition, reorganization, or sale of all or substantially all of the business, subject to continued protection of personal data consistent with this Statement.

The current list of subprocessors is published and is updated in accordance with the notice period set out in the DPA. As of the effective date of this Statement, DataTako engages the following principal subprocessors and third-party service providers:

Provider	Role	Location of processing
Hetzner Online GmbH	Infrastructure hosting (servers, primary database, application runtime)	Germany (EU)

Provider	Role	Location of processing
Stripe Payments Europe, Limited / Stripe, Inc.	Payment processing (acts as independent controller for payment-card data)	Ireland (EU) / United States
Twilio Inc. (SendGrid)	Transactional email delivery	United States
Microsoft Ireland Operations Limited / Microsoft Corporation	Power BI embedding, Microsoft Graph, Entra ID, Microsoft 365 SMTP relay (where used)	European Union and globally per Microsoft's data residency commitments
Functional Software, Inc. (Sentry)	Error and performance monitoring	United States
Google Ireland Limited	Google Analytics 4, Google Tag Manager, reCAPTCHA (only where the customer or user has activated the corresponding integration)	European Union and United States
Product Fruits s.r.o.	In-app product guidance and usage analytics	European Union
UserJot	Customer feedback collection	United States

Customers operating their own custom domain may additionally configure their own analytics tags (Google Analytics 4 and Google Tag Manager). In such cases, the customer is the controller for the personal data collected through those tags and is responsible for the lawful basis, transparency, and consent management with respect to the visitors to its custom-domain interface.

9. International data transfers

The Platform's primary application infrastructure and database are hosted with Hetzner Online GmbH in **Germany**, within the European Economic Area ("EEA"). Personal data processed for the core functioning of the Service is therefore stored within the EEA.

Certain subprocessors listed in Section 8 are established in, or may transfer personal data to, countries outside the EEA, in particular the United States. Where such transfers occur, DataTako relies on the following transfer mechanisms under Chapter V of the GDPR:

- The European Commission's adequacy decision for the **EU–U.S. Data Privacy Framework** (Commission Implementing Decision (EU) 2023/1795), where the recipient is certified under the Framework;
- The **Standard Contractual Clauses** (Commission Implementing Decision (EU) 2021/914), supplemented where necessary with additional technical, contractual, and organizational measures based on a transfer impact assessment;
- Other appropriate safeguards permitted under Articles 46–49 GDPR, where applicable.

A copy of the Standard Contractual Clauses concluded with a given subprocessor, and the related transfer impact assessment, is available to data subjects on reasoned request, with redactions where necessary to protect commercial confidentiality.

10. Security measures

DataTako implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in line with Article 32 GDPR. These include:

- **Encryption in transit** — TLS for all client–server, server–subprocessor, and inter-service communication.
- **Encryption at rest** — encryption of database storage volumes; encrypted storage of sensitive credential fields (for example, custom SMTP passwords and Power BI service-account passwords).
- **Authentication and access control** — JWT-based session management with short-lived access tokens and revocable refresh tokens; password storage as salted hashes; optional multi-factor authentication; configurable session inactivity timeout; configurable IP whitelisting at tenant level.
- **Single sign-on** — support for SAML 2.0 and Microsoft Entra ID, allowing customers to enforce their own authentication policies.
- **Tenant isolation** — multi-tenant architecture in which all tenant-scoped entities are filtered at the data-access layer so that requests are constrained to the tenant of the authenticated principal.
- **Audit logging** — recording of administrative and security-relevant actions, including impersonation events, with response status and duration.
- **Secure development practices** — code review, dependency management, secrets management, separation of staging and production environments.
- **Backups and disaster recovery** — regular backups of the production database with documented recovery procedures.
- **Personnel** — confidentiality undertakings, role-based access on a least-privilege basis, and security awareness training for staff with access to personal data.
- **Vulnerability and incident management** — monitoring, error tracking, and a documented procedure for handling personal data breaches, including notification to controllers and supervisory authorities within the timeframes required by Articles 33–34 GDPR.

In the event of a personal data breach affecting customer data, DataTako will notify the affected customer without undue delay in accordance with the DPA.

11. Rights of data subjects

Subject to the conditions set out in the GDPR, data subjects have the following rights in respect of their personal data:

- **Right of access** (Article 15) — to obtain confirmation as to whether personal data concerning them is being processed and, where so, a copy of that data and the related information.
- **Right to rectification** (Article 16) — to obtain rectification of inaccurate personal data and completion of incomplete personal data.
- **Right to erasure** (Article 17) — to obtain erasure of personal data in the cases set out in the GDPR.

- **Right to restriction of processing** (Article 18) — to obtain restriction of processing in the cases set out in the GDPR.
- **Right to data portability** (Article 20) — to receive the personal data the data subject has provided in a structured, commonly used, and machine-readable format, and to transmit it to another controller, where the processing is based on consent or contract and is carried out by automated means.
- **Right to object** (Article 21) — to object, on grounds relating to the data subject's particular situation, to processing based on legitimate interests, and to object at any time to processing for direct marketing.
- **Right not to be subject to automated decision-making** (Article 22) — DataTako does not carry out solely automated decision-making producing legal or similarly significant effects on data subjects within the meaning of Article 22 GDPR.
- **Right to withdraw consent** — where processing is based on consent, the data subject may withdraw consent at any time, without affecting the lawfulness of processing carried out before withdrawal.
- **Right to lodge a complaint** with a supervisory authority — in particular in the Member State of the data subject's habitual residence, place of work, or place of the alleged infringement. The competent supervisory authority for DataTako is the Autoriteit Persoonsgegevens (Netherlands), https://autoriteitpersoonsgegevens.nl.

Where the data subject is an end user provisioned within a customer's tenant, requests should in the first instance be directed to that customer as controller. DataTako will assist the customer in responding to such requests as set out in the DPA. Requests addressed to DataTako directly will be acknowledged and, where appropriate, forwarded to the relevant customer.

To exercise rights in respect of processing for which DataTako is the controller, data subjects may contact privacy@datatako.com. DataTako will respond within one month of receipt of the request, with the possibility of extending that period by two further months in accordance with Article 12(3) GDPR. DataTako may request additional information to verify the identity of the requester, in order to prevent unauthorized disclosure.

12. Cookies and similar technologies

The Platform uses cookies and equivalent client-side storage mechanisms for the following purposes.

12.1 Strictly necessary

These are required for the Platform to function and cannot be disabled without breaking core functionality. They are set on the basis of Article 6(1)(b) GDPR and the strictly-necessary exemption under the ePrivacy Directive.

- Authentication tokens (stored in browser local storage) used to maintain the user's session and to support automatic refresh of access tokens
- Session continuity tokens used for SSO and single-logout flows
- Security cookies set by reCAPTCHA on public forms to detect automated abuse

12.2 Functional

- User-interface preferences (language, layout)

- Tenant-resolution information for users connecting to a customer's custom domain

12.3 Analytics, product, and feedback

These technologies are activated where applicable and are subject to consent in accordance with Article 6(1)(a) GDPR and applicable national ePrivacy rules. They include:

- Sentry — error and performance monitoring for the frontend application
- Google Analytics 4 and Google Tag Manager — usage analytics, where DataTako or a customer (on a custom domain) has activated them
- Product Fruits — in-app guidance and feature analytics
- UserJot — in-app feedback collection

Users may manage their preferences at any time through the cookie consent interface presented on first use of the website.

Where a customer operates the Platform under its own custom domain and configures its own Google Analytics 4 or Google Tag Manager containers, the customer is the controller for the resulting cookies and is responsible for providing notice and obtaining consent from its visitors.

13. Contact

Topic	Contact
General inquiries	info@datatako.com
Privacy inquiries and rights requests	privacy@datatako.com
Security disclosures	security@datatako.com
Postal address	Antareslaan 65, 2132JE Hoofddorp
Data Protection Officer	security@datatako.com

Customers with an existing DPA may use the contact channels designated therein.

14. Updates to this Statement

DataTako may update this Statement from time to time to reflect changes in the Platform, in applicable law, or in the way personal data is processed. The "Effective date" and "Last updated" fields at the top of this Statement indicate when it was last revised. Material changes will be communicated to customers in advance through the Platform, by email to the registered administrative contact, or by another reasonable means, and where required will not take effect before the notice period set out in the DPA has elapsed. Continued use of the Platform after a revised Statement takes effect constitutes acknowledgement of the revised Statement; it does not, however, constitute consent where consent is required as a legal basis under the GDPR.