DATANYX DATA PROCESSING ADDENDUM

Tekizma Inc., DBA Datanyx
11921 Freedom Drive, Suite 550, Reston, VA 20190, United States
https://www.datanyx.com/legal/dpa-18-03-2026.pdf — legal@datanyx.com

This Data Processing Addendum ("DPA") forms part of, and is incorporated by reference into, the **Datanyx SaaS License Agreement** ("License Agreement") entered into between Tekizma Inc., DBA Datanyx ("Datanyx" or "Processor") and the Customer identified in the applicable Order Form ("Customer" or "Controller"). In the event of any conflict between this DPA and the License Agreement with respect to the processing of Personal Data, this DPA shall prevail.

This DPA applies to the SaaS deployment of the Datanyx platform and describes how Datanyx processes Personal Data in connection with the provision of the Services. This DPA applies only to the extent Datanyx processes Personal Data on behalf of Customer in the course of providing the Services.

1. DEFINITIONS

For the purposes of this DPA, the following definitions apply. Terms not defined here have the meaning given in the License Agreement or applicable data protection laws.

1.1. "Applicable Data Protection Laws" means all laws and regulations applicable to the processing of Personal Data under this DPA, including without limitation: the General Data Protection Regulation (EU) 2016/679 ("GDPR"); the UK General Data Protection Regulation and the Data Protection Act 2018 ("UK GDPR"); the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"); the Virginia Consumer Data Protection Act ("CDPA"); the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"), where applicable; and any other applicable national, federal, state, or provincial data protection or privacy laws.

1.2. "Controller" means the entity that determines the purposes and means of the processing of Personal Data. For the purposes of this DPA, Customer is the Controller.

1.3. "Customer Data" means any data, including Personal Data, that Customer submits to, uploads to, or causes to be processed by the Datanyx platform in connection with the Services.

1.4. "Data Subject" means the identified or identifiable natural person to whom Personal Data relates.

1.5. "Personal Data" means any information relating to an identified or identifiable natural person, as defined under Applicable Data Protection Laws.

1.6. "Processor" means the entity that processes Personal Data on behalf of the Controller. For the purposes of this DPA, Datanyx is the Processor.

1.7. "Processing" or "Process" means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organisation, storage, retrieval, adaptation, alteration, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.

1.8. "Security Incident" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by Datanyx.

1.9. "Subprocessor" means any third party engaged by Datanyx to process Personal Data on Datanyx's behalf in connection with the Services.

1.10. "Standard Contractual Clauses" or "SCCs" means, where applicable to transfers of Personal Data from the EEA to Datanyx in the United States or other third countries that have not received an EU adequacy decision, the standard contractual clauses adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as may be updated or replaced from time to time. SCCs are only relevant under this DPA to the extent that Applicable Data Protection Laws of the EEA or a Member State require their use for the lawful transfer of Personal Data.

2. ROLES OF THE PARTIES AND NATURE OF PROCESSING

2.1. Roles:

The parties acknowledge that, for the purposes of Applicable Data Protection Laws, Customer is the Controller and Datanyx is the Processor with respect to Personal Data contained in Customer Data. Datanyx processes Personal Data only on behalf of and in accordance with the documented instructions of Customer.

2.2. Processing Instructions:

This DPA and the License Agreement constitute Customer's complete and documented instructions to Datanyx for the processing of Personal Data. Datanyx will process Personal Data only in accordance with these instructions unless required to do so by applicable law, in which case Datanyx will notify Customer of that legal requirement before processing, unless such notification is prohibited by law.

Customer warrants that it has all necessary rights, consents, and authority to instruct Datanyx to process Personal Data as described in this DPA and the License Agreement, and that such instructions comply with Applicable Data Protection Laws.

2.3. Nature of the Datanyx SaaS Platform:

Datanyx provides a cloud-hosted data integration, analytics, and visualisation platform (the "SaaS Platform") that enables Customers to connect to their own data sources, load and transform data, generate dashboards and reports, and schedule automated report delivery. All Customer Data processed under this DPA is handled within Datanyx-managed cloud infrastructure. Datanyx maintains appropriate technical and organisational measures to protect Customer Data within that environment.

The Datanyx SaaS Platform supports the following data processing modes, each of which may involve Personal Data depending on the data Customer connects to or loads into the platform:

2.4. Direct Connect:

Where Customer uses the Direct Connect configuration, queries are executed directly against Customer-controlled data sources (such as databases, data warehouses, or data lakes). Query results are temporarily cached within Datanyx-managed infrastructure solely to support the performance of the platform and the Customer's active session. Datanyx does not store Customer Data under this mode. The cache is cleared on a daily basis or on an ad hoc basis. No Customer Data is written to persistent storage under this mode.

2.5. Data Load:

Where Customer uploads, ingests, or imports Customer Data into the Datanyx platform, that data is stored in Datanyx-managed persistent storage within the SaaS infrastructure. Data Load enables customers to work with data directly within the platform without requiring a live connection to the source system. Customer Data stored under this mode remains in Datanyx-managed infrastructure for as long as the Customer retains it or until deleted in accordance with Section 10 of this DPA. Datanyx's full security, retention, and deletion obligations under this DPA apply to all Customer Data stored through Data Load.

2.6. Data Transformations and Pipelines:

Where Customer configures data transformation jobs or data pipelines within the platform, Customer Data is loaded into temporary compute memory within Datanyx-managed infrastructure for the duration of the job execution. Once the job completes, the data is cleared from temporary memory. The output generated by a job is written to a destination as per the Customer's configuration. Such output is not automatically persisted within the Datanyx platform and Datanyx's retention and deletion obligations under Section 10 apply only to the extent output is written to Datanyx-managed storage as part of that configuration.

2.7. Scheduled Reports:

Where Customer configures scheduled reports, the Datanyx platform generates report outputs on the defined schedule. These outputs, which may contain Customer Data including Personal Data, are stored in Datanyx-managed cloud object storage (Amazon Web Services S3 or equivalent).

Report outputs persist in storage until deleted by the Customer or until the end of the applicable retention period set out in Section 10. Datanyx's full security, retention, and deletion obligations under this DPA apply to all report outputs stored in Datanyx-managed infrastructure.

3. CUSTOMER OBLIGATIONS

Customer is solely responsible as Controller for:

- Ensuring that its collection, use, and transfer of Personal Data to Datanyx complies with Applicable Data Protection Laws, including obtaining all necessary consents and providing all required notices to Data Subjects;
- Determining the lawful basis for processing Personal Data and ensuring that basis remains valid throughout the term of this DPA;
- Ensuring the accuracy, quality, and legality of the Personal Data submitted to the Services;
- Configuring access permissions and data source connections within the Datanyx platform;
- Determining which data processing modes (Direct Connect, Data Load, Transformations, Scheduled Reports) are used and ensuring that such use is consistent with Customer's obligations under Applicable Data Protection Laws;
- Notifying Datanyx promptly in writing of any changes to applicable processing instructions.

4. DATANYX OBLIGATIONS AS PROCESSOR

4.1. Compliance: Datanyx will process Personal Data only in accordance with Customer's documented instructions and as required by Applicable Data Protection Laws. Datanyx will promptly notify Customer if, in Datanyx's reasonable opinion, any instruction from Customer would violate Applicable Data Protection Laws.

4.2. Confidentiality of Processing: Datanyx will ensure that all personnel authorised to process Personal Data are subject to binding confidentiality obligations and receive appropriate training on data protection. Access to

Personal Data is restricted to personnel who require it for the purpose of providing the Services.

4.3. No Selling or Independent Use: Datanyx will not sell, rent, lease, or disclose Personal Data to any third party for that third party's own purposes. Datanyx will not use or process Personal Data for advertising, profiling, independent analytics, or any purpose other than providing the Services to Customer.

4.4. Assistance with Data Subject Rights: Taking into account the nature of the processing, Datanyx will provide reasonable assistance to Customer in fulfilling its obligations to respond to Data Subject requests exercising rights under Applicable Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, and objection). Where Datanyx receives a Data Subject request directly, it will promptly refer that request to Customer without responding to it directly, unless required by law.

4.5. Assistance with Compliance Obligations: Datanyx will provide reasonable assistance to Customer in ensuring compliance with Customer's obligations under Applicable Data Protection Laws with respect to security of processing, notification of Security Incidents, data protection impact assessments, and prior consultation with supervisory authorities, taking into account the nature of processing and the information available to Datanyx. To the extent legally permitted, Customer shall be responsible for any costs arising from assistance that requires material effort or resources beyond Datanyx's standard support obligations.

5. CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS

The categories of Personal Data processed and the categories of Data Subjects are determined by Customer in its capacity as Controller. Depending on Customer's configuration and use of the Services, Datanyx may process Personal Data relating to the following categories of Data Subjects and Personal Data:

Category	Details
Data Subjects	Customer's employees, contractors, clients, patients, or other individuals whose data Customer processes through the Services
Categories of Personal Data	May include: names, contact details, identification numbers, professional information, financial data, operational data, healthcare or medical data (if applicable), and analytics datasets, depending on Customer's use of the platform
Sensitive Data	Datanyx does not require the submission of sensitive personal data (including health data, racial or ethnic origin, political opinions, religious beliefs, genetic or biometric data) to provide the Services. If Customer submits sensitive data, Customer does so at its own election and is solely responsible for ensuring an appropriate lawful basis exists for such processing
Purposes of Processing	Connecting to Customer data sources; retrieving, transforming, and analysing datasets; generating dashboards and visualisations; executing Customer-requested data operations; providing platform support and maintenance
Duration of Processing	For the term of the License Agreement and for the period necessary to fulfil deletion or return obligations following termination

6. SECURITY MEASURES

Datanyx will implement and maintain appropriate technical and organisational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. These measures take into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risks to Data Subjects.

6.1. Technical measures may include, without limitation:

- Encryption of data in transit using industry-standard TLS protocols
- Encryption of data at rest within Datanyx-managed infrastructure (SaaS deployments)
- Role-based access controls and least-privilege access policies
- Multi-factor authentication for access to platform administration systems
- Security monitoring, logging, and audit trails
- Vulnerability management and regular security assessments
- Secure software development practices

6.2. Organisational measures may include, without limitation:

- Data protection training for all personnel with access to Personal Data
- Binding confidentiality obligations for all authorised personnel
- Incident response and Security Incident management procedures
- Vendor and Subprocessor security assessments

6.3. Ephemeral Processing Modes: For Customer Data processed through Direct Connect mode, data is held only in temporary cache within Datanyx-managed infrastructure and is not written to persistent storage. Datanyx's at-rest encryption and persistent storage security obligations under this Section 6 apply specifically to Customer Data stored through Data Load and Scheduled Reports modes.

6.4. Security Updates: Datanyx may update or modify its security measures from time to time. Datanyx will use commercially reasonable efforts to maintain an equivalent or improved overall level of protection and will not materially decrease the overall security of the Services.

7. SECURITY INCIDENTS

7.1. Notification: In the event that Datanyx becomes aware of a confirmed Security Incident affecting Personal Data processed on behalf of Customer, Datanyx will notify Customer without undue delay and, where feasible, within

seventy-two (72) hours of becoming aware of the Security Incident, to the extent such notification is practicable.

7.2. Content of Notification: Datanyx's notification will include, to the extent known at the time:

- A description of the nature of the Security Incident, including the categories and approximate number of Data Subjects and records affected;
- The name and contact details of Datanyx's data protection contact;
- The likely consequences of the Security Incident;
- The measures taken or proposed to address the Security Incident and mitigate its effects.

Datanyx may provide this information in phases if not all information is available at the time of initial notification. Datanyx will promptly provide Customer with additional information as it becomes available.

7.3. Customer Responsibilities: Customer is solely responsible for determining whether the Security Incident triggers any notification obligations to Data Subjects or supervisory authorities under Applicable Data Protection Laws, and for making any such notifications.

7.4. Scope: This Section 7 applies to Security Incidents caused by or occurring within Datanyx-managed systems and infrastructure. Customer is solely responsible for identifying, managing, and reporting any security incidents occurring within Customer-controlled systems, networks, or data sources.

8. SUBPROCESSORS

8.1. Authorised Subprocessors: Customer provides general written authorisation for Datanyx to engage Subprocessors to assist in the provision of the Services, subject to the conditions in this Section 8. Datanyx will make available to Customer a current list of Subprocessors upon written request.

8.2. Subprocessor Requirements: Datanyx will ensure that each Subprocessor is bound by written data processing obligations that impose

data protection requirements no less protective than those set out in this DPA. Datanyx remains responsible for the acts and omissions of its Subprocessors to the same extent as if Datanyx had performed the processing directly.

8.3. Changes to Subprocessors: Datanyx will provide Customer with reasonable prior notice of any intended addition or replacement of a Subprocessor. Customer may object to a new Subprocessor on reasonable data protection grounds by notifying Datanyx in writing within fourteen (14) days of receiving notice. If Customer objects and Datanyx cannot accommodate the objection, either party may terminate the relevant Services on written notice without liability for such termination.

8.4. Current Subprocessors: Details of current Subprocessors engaged by Datanyx are available to Customer upon written request to legal@datanyx.com.

9. DATA SUBJECT RIGHTS

Customer, as Controller, is responsible for responding to Data Subject requests under Applicable Data Protection Laws. Datanyx will:

- Promptly refer to Customer any Data Subject request received by Datanyx without responding to it directly, unless required by law;
- Provide Customer with reasonable technical assistance to facilitate Customer's response to Data Subject requests, including access, rectification, erasure, restriction, portability, and objection, to the extent the requested action relates to Personal Data within Datanyx's systems;
- Not respond to Data Subject requests on behalf of Customer except as instructed by Customer in writing or as required by applicable law.

Datanyx may charge a reasonable fee for assistance that requires significant effort or resources, and will notify Customer of any such fee before incurring it.

10. RETENTION AND DELETION

10.1. During the Term: Datanyx will retain Customer Data only for as long as necessary to provide the Services or as required by applicable law. Retention obligations vary by processing mode as set out below.

10.2. Direct Connect Mode — No Persistent Storage: Customer Data processed through Direct Connect mode is held only in temporary cache for the duration of the active session and is cleared on a daily basis or ad hoc. No persistent storage occurs under this mode and accordingly no deletion action by Datanyx is required on termination for data processed exclusively through Direct Connect.

10.3. Persistent Processing Modes — Data Load and Scheduled Reports: Customer Data stored through Data Load or Scheduled Reports modes is retained in Datanyx-managed persistent storage (including Amazon Web Services S3 for report outputs) for as long as the Customer retains it within the platform or until the License Agreement terminates or expires. Upon termination or expiration, Datanyx will, at Customer's election, either: (a) make Customer Data available for Customer to download or export for a period of thirty (30) days following termination; or (b) securely delete or destroy Customer Data in Datanyx's possession or control using commercially reasonable means, except to the extent Datanyx is required by applicable law to retain a copy. Customer Data held in automated backup systems will be overwritten or deleted within ninety (90) days following the deletion of the primary data.

10.4. Certification: Upon Customer's written request, Datanyx will provide written confirmation that deletion procedures have been carried out in accordance with this Section 10 with respect to Customer Data held in persistent storage.

11. AUDITS AND ASSESSMENTS

11.1. Audit Rights: Upon Customer's reasonable written request, Datanyx will make available all information reasonably necessary to demonstrate compliance with its obligations under this DPA and under Applicable Data Protection Laws.

11.2. Audit Conditions: Audits shall be conducted no more than once per calendar year, on reasonable prior written notice, during normal business

hours, and in a manner that does not unreasonably disrupt Datanyx's operations. Datanyx may satisfy its audit obligations by providing Customer with relevant third-party certifications or audit reports where available.

11.3. Data Protection Impact Assessments: Where required under Applicable Data Protection Laws, Datanyx will provide reasonable assistance to Customer in conducting data protection impact assessments relating to the use of the Services, to the extent such assessments require information within Datanyx's possession or control.

12. INTERNATIONAL DATA TRANSFERS

12.1. General: Datanyx may process Personal Data in jurisdictions where Datanyx or its Subprocessors operate, including the United States. Where Applicable Data Protection Laws restrict the transfer of Personal Data to other countries, Datanyx will put in place appropriate safeguards to ensure compliance.

12.2. Cross-Border Transfers: Where Customer is subject to data transfer restrictions under applicable law and Personal Data is transferred to Datanyx outside the originating jurisdiction, Datanyx will, upon Customer's written request, implement appropriate transfer mechanisms including, where required, the Standard Contractual Clauses or such other safeguards as applicable law recognises. Datanyx will cooperate with Customer to execute any required documentation.

12.3. HIPAA: Where Customer processes Protected Health Information ("PHI") as a Covered Entity or Business Associate under HIPAA, the parties must execute a separate Business Associate Agreement ("BAA") before any PHI is submitted to the Services. Customer must not submit PHI unless a BAA is in place.

12.4. CCPA/CPRA: To the extent the CCPA/CPRA applies, Datanyx acts as a Service Provider and will not sell or share Personal Data received from Customer, will not use or disclose it for any purpose other than providing the Services, and will not combine it with data from other sources except as the CCPA/CPRA permits.

13. TERM

This DPA is effective from the date the License Agreement is entered into and remains in force for the duration of the License Agreement. Termination or expiry of the License Agreement automatically terminates this DPA, subject to the survival of any post-termination obligations set out herein, including data deletion and confidentiality obligations.

14. LIABILITY

Each party's liability under this DPA is subject to the limitations and exclusions set out in the applicable License Agreement. The total aggregate liability of either party under this DPA shall not exceed the liability cap set out in the License Agreement. Nothing in this DPA is intended to increase or extend either party's liability beyond what is permitted under the License Agreement, except to the extent required by Applicable Data Protection Laws.

15. GOVERNING LAW

This DPA is governed by and construed in accordance with the laws of the Commonwealth of Virginia, USA, consistent with the License Agreement, except to the extent that Applicable Data Protection Laws of another jurisdiction mandate otherwise. Any dispute arising out of or relating to this DPA shall be resolved in accordance with the dispute resolution provisions of the applicable License Agreement.

16. ORDER OF PRECEDENCE

In the event of any conflict or inconsistency between this DPA and the License Agreement with respect to the processing of Personal Data and privacy obligations, the terms of this DPA shall prevail. For all other matters, the order of precedence set out in the License Agreement applies.

SCHEDULE 1 — DETAILS OF PROCESSING

Nature and Purpose of Processing: Datanyx processes Personal Data as a Processor on behalf of Customer solely to provide the SaaS Services. Processing occurs across the following modes: (1) Direct Connect — real-time querying of Customer-controlled data sources, with data held only in volatile memory; (2) Data Load — ingestion and persistent storage of

Customer-uploaded data in Datanyx-managed infrastructure; (3) Data Transformations and Pipelines — transformation of Customer Data in temporary compute memory, with outputs persisted if saved to the platform; and (4) Scheduled Reports — automated generation and storage of report outputs in Datanyx-managed cloud object storage (AWS S3 or equivalent).

Duration: For the term of the License Agreement, plus any post-termination retention period required by applicable law or set out in Section 10 of this DPA.

Categories of Data Subjects: As described in Section 5 of this DPA, as determined by Customer.

Categories of Personal Data: As described in Section 5 of this DPA, as determined by Customer.

Processor (Datanyx): Tekizma Inc., DBA Datanyx, 11921 Freedom Drive, Suite 550, Reston, VA 20190, United States. Contact: legal@datanyx.com.

Controller (Customer): As identified in the applicable Order Form.

SCHEDULE 2 — SECURITY MEASURES

The technical and organisational security measures maintained by Datanyx are as described in Section 6 of this DPA. Datanyx will maintain and update its security measures in accordance with industry standards. Customers may request a summary of Datanyx's current security certifications and audit reports by contacting legal@datanyx.com.

Measure	Description
Encryption in Transit	TLS 1.2 or higher for all data in transit between Customer and Datanyx systems
Encryption at Rest	AES-256 encryption for Customer Data stored within Datanyx-managed infrastructure (SaaS)

Measure	Description
Access Controls	Role-based access control (RBAC) with least-privilege principles; multi-factor authentication for administrative access
Authentication	Secure credential management; support for Single Sign-On (SSO) where Customer configures it
Monitoring and Logging	Security event logging and monitoring; anomaly detection; audit trails for administrative actions
Vulnerability Management	Regular security assessments; penetration testing; patch management procedures
Incident Response	Documented Security Incident response plan; designated security contact; 72-hour notification commitment
Personnel	Data protection training for all personnel; binding confidentiality obligations; background screening where applicable
Physical Security	Datanyx-managed infrastructure is hosted in data centres with appropriate physical security controls (SaaS)