Precisely Data Integrity Suite Privacy Datasheet

Precisely Global Privacy Office

Version 1.0

Precisely Data Integrity Suite Privacy Datasheet

The purpose of this Datasheet is to provide Precisely customers with information relating to how personal data may be captured, processed and stored by and within Precisely Data Integrity Suite products and services.

1. Product Summary

Application

The Data Integrity Suite provides a robust web interface designed for data governance and data quality teams. Through this platform, users can seamlessly discover datasets, enforce governance policies, and apply data quality rules across organizational data assets. The Data Integrity Suite web application includes an integrated database that securely stores data imported via Data Connection configurations established by Precisely customers. This ensures that critical data remains accessible for governance and quality management within the platform.

Core Capabilities

The Data Integrity Suite is a **interoperable suite of SaaS services** designed to ensure trusted data across the customer's enterprise. It includes:

- **Data Integration:** Connect and synchronize data from diverse sources, including mainframe, hybrid, and cloud environments.
- **Data Observability:** Monitor data health and lineage to detect anomalies and ensure reliability.
- **Data Quality & Governance:** Apply rules and policies to maintain accuracy and compliance.
- **Data Enrichment:** Enhance datasets with curated attributes like demographics, property details, and geospatial intelligence.
- **Geo Addressing & Spatial Analytics:** Validate, geocode, and analyze location-based data for advanced insights.

Architecture & Deployment

Data Integrity Suite Services

- **Data Integrity Foundation:** Provides essential building blocks like connectors, cataloging, and workflow orchestration.
- **Security & Administration:** Centralized controls for safe operations and usage tracking.
- **Data Products & APIs:** The Suite includes APIs for address validation, geocoding, email/phone verification, and property lookups. These APIs enable real-time data validation and enrichment for customer-facing and internal applications. Examples:
    - I. Address Autocomplete API
    - II. Address Verify API
    - III. GeoTAX API
    - IV. Email Verification API
    - V. Data Graph API
- **Flexible Deployment:** Works on-premises, in private clouds, or multi-cloud environments.
- **Interoperability:** Integrates with enterprise systems (ERP, CRM, BI tools) and analytics platforms.
- **AI-Powered Intelligence:** Offers AI-driven recommendations and automation for workflows.

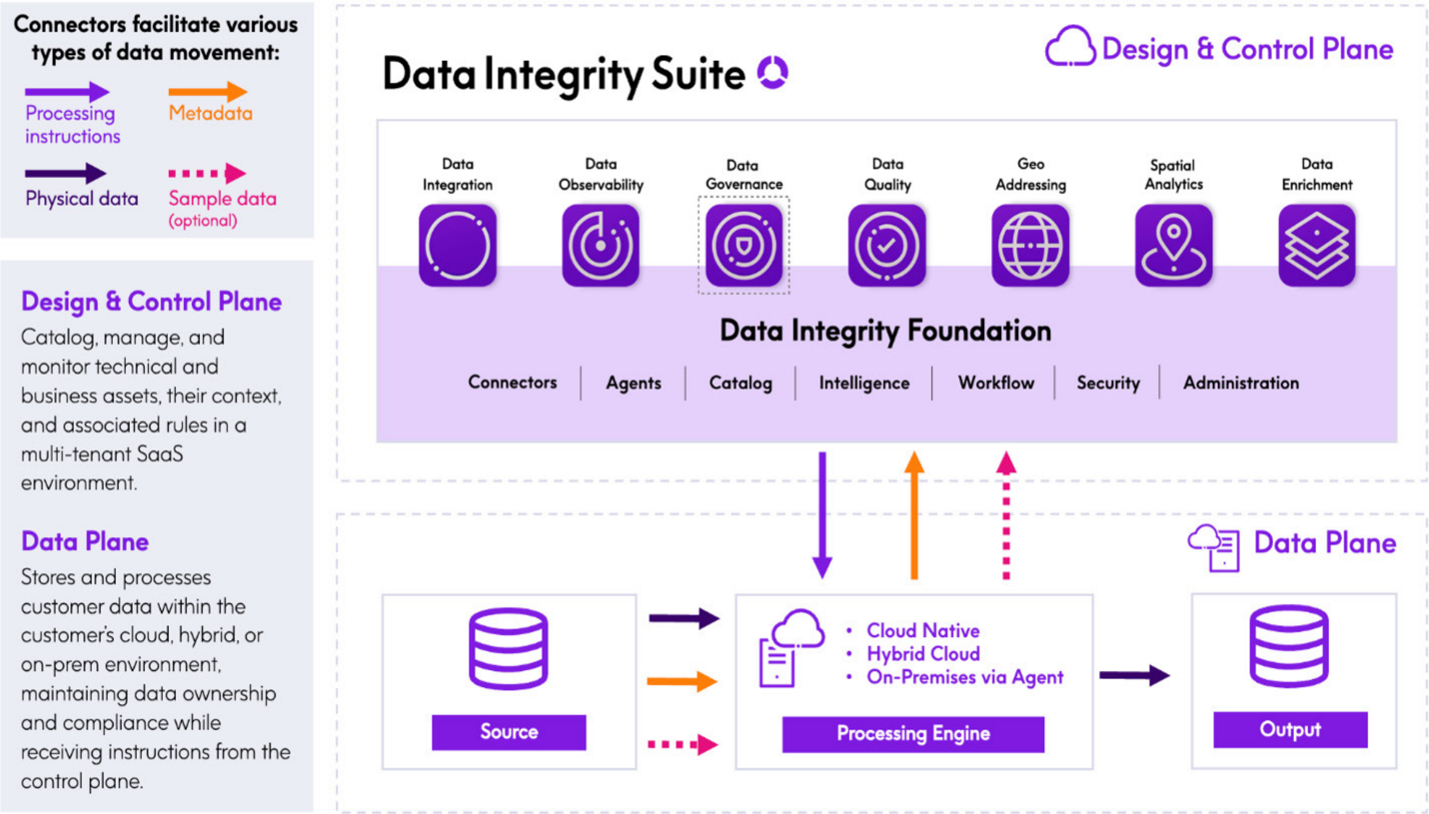
The Data Integrity Suite operates as a **cloud-based control plane**, orchestrating data management tasks while ensuring maximum security and control. Data processing occurs as close to the source as possible—either within the originating system or, for on-premises environments, through a **customer-managed** deployment behind the firewall.

The Data Integrity Suite installed within the customer's infrastructure leverages Precisely connectors to access approved data sources. It executes **discovery and integration tasks locally**, ensuring that all customer data remains within the customer's environment and under their control.

The customer fully manages configuration of tasks and connections. Precisely does **not require direct access** to customer systems. Only minimal metadata (Data Output)—such as job status and configuration details—is exchanged with the cloud service to coordinate and monitor operations.

Information flow map for the Data Integrity Suite

The information flow map detailed below for the Suite identifies where information is collected, stored, accessed, processed, and transferred. Please note the specifics of this information flow map depend on the components and deployment methods selected by our customers.



Design & Control Plane

Catalog, manage, and monitor technical and business assets, their context, and associated rules in a multi-tenant SaaS environment.

Data Plane

Stores and processes customer data within the customer's cloud, hybrid, or on-prem environment, maintaining data ownership and compliance while receiving instructions from the control plane.

Locations/regions where customer data is processed

USA, Europe (including Ireland and the UK),
Asia Pacific (Australia)

Note: the Data Integrity Suite provides customers with the ability to select preferred data hosting regions during initial provisioning.

Sub-processors who share responsibility of processing

Data360 Analyze, Data360 Govern, Smart Data Platform (SDP), AWS (hosting provider), Mongo DB (hosting provider), Temporal (hosting provider), LogRocket (customer support), Heap (customer support)

2. Customer Data Types

The Data Integrity Suite provides two processing models. The most applied model (Model 1) has the services running in the customer environment with no movement of customer data to Precisely.

Model 1: Processing in your environment

For the services referenced below, the Suite uses in-place processing. Workloads run within the customer's own data platforms, for example Snowflake, Databricks, and SQL based systems. Customer data does not leave the customer's environment for these services, and Precisely receives only the limited metadata described above (Data Output).

Services:

- Data Catalog
- Data Governance
- Data Observability
- Data Quality Pipeline
- Data Integration

Model 2: Processing through Precisely APIs

Location Intelligence and Spatial Analytics are accessed through APIs. For these services, the customer sends the relevant data to Precisely for processing, for example geocoding, enrichment, or spatial analysis, and receives results in return. Details of data handling for these API based services including transmission, retention, and deletion follow the customer agreement and service configuration.

For API-based services, limited customer data such as address information, email addresses, telephone numbers and other non-sensitive datasets may be inputted by customers through these APIs to use the Data Integrity Suite services. Precisely processes these datasets that are provided by our customers to produce the requested results and return those results to the customer.

Access and login requirements

To access the Data Integrity Suite, users sign in with an authenticated account, typically a business email provided by their organization. The Suite uses role-based access to manage permissions within the application. Single sign-on and multi-factor authentication are configured and controlled by the customer through their identity provider.

3. Access to Personal data

Customer Access

Customers have access to their respective workspaces and can grant individual access to users within their workspaces. The Data Integrity Suite supports role-based security, where users within a customer workspace can only see and access the data and items the customer approves of them. Customer data is segmented to the customer workspace/tenant of the Suite. We maintain strict separation of customer data; it is never combined with data from other customers.

Customers' retain full control over data sharing. If a customer elects not to submit sample data via the Suite, Precisely will not have access to such data. Data visibility is entirely dependent on the customer's configuration choices.

Precisely Access to Customer Data: Data Submission Configuration

The availability of data within the Data Integrity Suite is governed by submission settings configured by the customer's system administrator. These settings determine which file types and session data, if any, are uploaded to the Suite platform.

During customer support and monitoring, customer data is isolated within each customer's workspace. Data Integrity Suite support teams do not have direct access to customer workspaces. Our support and monitoring practices are designed to protect privacy and security. When assistance is requested, support may review limited diagnostic information (such as system logs) only with the customer's explicit authorization. Monitoring tools are used to maintain system health and performance and are configured to avoid exposure to customer content.

4. Procedures for maintaining Customer Privacy

Data Ingestion Capabilities

The Data Integrity Suite supports ingestion of both Personal Data (aka Personally Identifiable Information [PII]) and non-Personal Data (aka non-PII). Supported data types and categories are customer-defined and may vary across implementations.

Data Sensitivity and Encryption

Due to the customer-controlled nature of the data input, Precisely applies robust encryption protocols to all ingested data—regardless of sensitivity classification. This ensures comprehensive protection of customer data throughout the Data Integrity Suite platform.

Hosting and Sub-Processor Access

Hosting services are provided by authorized sub-processors who may have access to customer data. All data is encrypted in transit and at rest, with encryption keys managed exclusively by Precisely, ensuring data protection and integrity.

Customer-Defined Hosting Locations (Data Residency)

The Data Integrity Suite provides customers with the ability to select preferred data hosting regions during initial provisioning. This flexibility supports compliance with local data residency regulations, including GDPR and other jurisdiction-specific requirements.

5. Compliance with Privacy Regulations

Precisely's Role as Processor or Controller

Precisely may act as either a data processor or a data controller depending on how the Data Integrity Suite is used. The role varies by service and by the type of data involved.

Processor Role

Precisely acts as a **data processor** when it handles personal data **solely to provide the Data Integrity Suite services** and only according to the customer's instructions. This applies to services where customers transmit data to Precisely systems for processing, including geocoding, enrichment, and spatial analytics (Model 2). When acting as a processor, processing is governed by the **Precisely Data Processing Addendum (DPA)**, which describes how customer data is handled, protected, and deleted.

Controller Role

Precisely acts as a **data controller** in situations where it determines how and why certain information is processed for its own business operations. This includes:

- **Account setup and service delivery:** Processing basic business contact information for billing, license management, service analytics, product improvement, and operational reporting.
- **Processing limited metadata:** When using Data Integrity Suite services that run entirely in the customer's environment, Precisely receives only **limited metadata** (e.g., logs, service configuration details, performance data). This metadata is used by Precisely for internal operational purposes such as service quality, diagnostics, and product improvement.

In these cases, Precisely is not processing the data on behalf of the customer, so a DPA is **not required**.

Summary of Roles by Deployment Model

Deployment Model	Description	Precisely Role	DPA Required?
Model 1: Processing in Customer Environment	All workloads run in the customer's own data platforms; Precisely receives only limited metadata.	**Controller** (for metadata only)	**No**
Model 2: Precisely API Processing	Customer sends data to Precisely for processing and receives results back.	**Processor**	**Yes**

The Precisely online DPA can be accessed via our Trust Center and here.

Customer Data Retention

During contract termination, the respective customer tenant is marked for deletion, and the data is deleted after the locking period. The data remains in the backup until the backup is expired.

Customer data is retained for as long as necessary to fulfil the purposes for which it was collected and processed. Precisely returns or destroys customer data upon customer request, or generally, in line with statutory record retention requirements. For further details on Precisely's data retention practices, please refer to the Precisely DPA and our Trust Center.

Compliance with Privacy Regulations

Our goal is to meet the requirements of all applicable privacy and data protection laws and regulations. This includes working to implement Privacy-by-Design and Default practices in the development of our products to address GDPR and CCPA requirements. Our obligations are further defined in our DPA, our Global Privacy Notice and our Trust Center.

Cross-Border Data Transfers

Precisely is a global business and so customer data may be processed in various countries. In the event of a need to share logs or customer data between different Precisely global sites, we put in place appropriate safeguards to protect customer personal data. For more information about our privacy practices, including Cross-Border Data Transfers, please see our Trust Center.

Security (Technical & Organizational Measures)

We use a combination of administrative, technical, and physical safeguards designed to help prevent unauthorized access and maintain data security. For more information about our data security practices, including our Technical and Organizational Measures, please see our DPA, Trust Center, and our Global Privacy Notice.

Disaster Recovery

Precisely's Disaster recovery strategy involves replicating data to another region within the same geopolitical area, with near real-time replication for S3 data and hourly for Mongo snapshots.

Our Global Privacy Office and Program

Precisely's Global Privacy Office, led by our Chief Privacy Officer, is involved throughout the design, architecture, and development of Precisely's products, processes, and solutions, in line with internationally recognized Privacy by Design principles. Our products and solutions are designed with global privacy and data protection laws at the forefront, including the EU and UK General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), as amended, and other applicable domestic and international data protection regulations.

For more information about Precisely's privacy practices, please see our Global Privacy Notice or visit our Trust Center.

About This Datasheet

The information provided within this Privacy Datasheet is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

Copyright Statement
Version 1.0
Last Update: 25 November 2025

1700 District Ave #300
Burlington, MA 01803
USA

precisely.com