# UserDesk

Data Processing Agreement

Between the Customer (Controller) and Prismatic Solutions (Processor)

**DRAFT — FOR REVIEW ONLY — NOT YET EXECUTED**

This Data Processing Agreement ("**DPA**") forms part of the service agreement (the "**Agreement**") between the entity identified in the signature block below (the "**Controller**") and Prismatic Solutions, operating as UserDesk (the "**Processor**"), for the provision of the UserDesk Microsoft 365 user management delegation service (the "**Service**").

This DPA is entered into to ensure compliance with applicable data protection laws, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the UK General Data Protection Regulation, and the Swiss Federal Act on Data Protection.



## 1. DEFINITIONS

**"Controller"**
The entity that determines the purposes and means of the Processing of Personal Data, as identified in the signature block of this DPA.

**"Processor"**
Prismatic Solutions, operating as UserDesk, which processes Personal Data on behalf of the Controller to provide the Service.

**"Data Subject"**
An identified or identifiable natural person whose Personal Data is processed under this DPA. In the context of the Service, Data Subjects are the Controller's employees and IT staff who use Microsoft 365.

**"Personal Data"**
Any information relating to a Data Subject that is processed by the Processor on behalf of the Controller in connection with the Service.

**"Processing"**
Any operation or set of operations performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, restriction, erasure, or destruction.

**"Sub-processor"**
Any third party engaged by the Processor to process Personal Data on behalf of the Controller.

**"Supervisory Authority"**
An independent public authority established by an EU/EEA Member State, the UK, or Switzerland to monitor the application of data protection laws.

**"GDPR"**
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as applicable, including the UK GDPR and Swiss equivalent.

**"SCCs"**
The Standard Contractual Clauses for the transfer of personal data to third countries, as adopted by the European Commission in Decision (EU) 2021/914.

**"Data Breach"**
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

## 2. SCOPE AND PURPOSE

### 2.1 Nature of Processing

The Processor processes Personal Data on behalf of the Controller solely for the purpose of providing the Service. The nature of processing includes the storage and management of Microsoft 365 user account metadata, maintenance of audit logs, and management of subscription and billing data.

### 2.2 Categories of Data Subjects

The Personal Data processed relates to the following categories of Data Subjects:

- The Controller's employees, contractors, and IT staff who use or are managed through Microsoft 365.
- The Controller's administrators who access the UserDesk portal.

### 2.3 Types of Personal Data

The Processor processes the following types of Personal Data:

- Names and email addresses (from Microsoft Entra ID profiles).
- Microsoft Entra ID tenant identifiers and user object identifiers.
- Portal roles (Admin, Member, Viewer) assigned within UserDesk.
- Audit log entries recording actions taken through the Service (who, what, when).
- Subscription status and billing information (managed through Stripe).
- User templates (saved configurations for creating new Microsoft 365 users).

### 2.4 Duration of Processing

The Processor shall process Personal Data for the duration of the Agreement. Upon termination of the Agreement, the Processor shall delete all Personal Data within thirty (30) days, unless retention is required by applicable law.

## 3. OBLIGATIONS OF THE PROCESSOR

### 3.1 Instructions

The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law. In such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless prohibited by law.

### 3.2 Confidentiality

The Processor shall ensure that all persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 3.3 Security Measures

The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as described in Annex II (Section 6) of this DPA.

### 3.4 Sub-processing

The Processor shall not engage another processor (Sub-processor) without prior specific or general written authorization of the Controller. The current list of authorized Sub-processors is set forth in Section 4 of this DPA.

### 3.5 Data Subject Rights

The Processor shall assist the Controller, by appropriate technical and organizational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights under the GDPR (access, rectification, erasure, restriction, portability, and objection).

### 3.6 Data Protection Impact Assessments

The Processor shall assist the Controller with data protection impact assessments (DPIAs) and prior consultation with Supervisory Authorities where required under Articles 35 and 36 of the GDPR.

### 3.7 Deletion or Return of Data

At the choice of the Controller, the Processor shall delete or return all Personal Data to the Controller after the end of the provision of the Service, and delete existing copies unless applicable law requires storage of the Personal Data.

### 3.8 Demonstration of Compliance

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this DPA, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

## 4. SUB-PROCESSORS

The Controller provides general written authorization for the Processor to engage the following Sub-processors. The Processor shall inform the Controller of any intended changes to the list of Sub-processors by email at least thirty (30) days in advance, giving the Controller the opportunity to object to such changes.

| Sub-processor | Location | Purpose |
|---|---|---|
| Vercel Inc. | United States | Application hosting and content delivery network (CDN) |

| | | |
|---|---|---|
| Supabase Inc. | United States (AWS us-east-1) | PostgreSQL database hosting for portal metadata and audit logs |
| Stripe Inc. | United States | Subscription payment processing |
| Resend Inc. | United States | Transactional and marketing email delivery |
| Microsoft Corporation | United States / Global | Microsoft Graph API access using Controller's own delegated OAuth tokens |

**Note:** Microsoft Graph API calls are made using the Controller's own delegated OAuth tokens. The Processor does not maintain standing access to the Controller's Microsoft 365 tenant.

## 5. INTERNATIONAL DATA TRANSFERS

All Processing of Personal Data by the Processor and its Sub-processors occurs in the United States. For transfers of Personal Data from the European Economic Area (EEA), the United Kingdom, or Switzerland to the United States, the parties rely on the Standard Contractual Clauses (SCCs) adopted by the European Commission in Implementing Decision (EU) 2021/914.

- Module Two (Controller to Processor) of the SCCs shall apply.
- The governing law for the SCCs shall be the laws of the EU Member State in which the Controller is established.
- The competent Supervisory Authority shall be the authority of the EU Member State in which the Controller is established.
- Sub-processors maintain their own SCCs, data processing addenda, or equivalent safeguards for international transfers.

## 6. DATA SECURITY MEASURES (ANNEX II)

The Processor implements the following technical and organizational measures to protect Personal Data, as required by Article 32 of the GDPR:

### 6.1 Technical Measures

- TLS 1.2+ encryption for all data in transit between clients, servers, and databases.
- Database encryption at rest provided by Supabase (AWS infrastructure).
- Row-level security (RLS) enabled on all database tables, restricting direct database access to authorized application roles only.
- OAuth access tokens and refresh tokens are stored exclusively in encrypted, HttpOnly, Secure, SameSite browser session cookies. Tokens are never written to the database or application logs.
- Rate limiting on all public-facing API endpoints to prevent abuse and enumeration attacks.
- Security headers applied to all HTTP responses: X-Frame-Options (DENY), X-Content-Type-Options (nosniff), Referrer-Policy (strict-origin-when-cross-origin), X-XSS-Protection, and Permissions-Policy.
- Role-based access control (RBAC) with three tiers: Admin, Member, and Viewer, each with distinct permissions.
- Immutable audit trail recording every action taken through the Service, including the actor, action, target, and timestamp.
- HTML sanitization on all user-provided content to prevent cross-site scripting (XSS) in emails and rendered pages.

### 6.2 Organizational Measures

- Access to production systems and databases is limited to authorized personnel of the Processor only.
- Regular security reviews of application code, dependencies, and infrastructure configuration.
- Documented incident response procedures for identifying, containing, and remediating security incidents.
- Due diligence on all Sub-processors, including review of their security practices and data protection commitments.
- Principle of least privilege applied to all system access and API permissions.

## 7. DATA BREACH NOTIFICATION

### 7.1 Notification

The Processor shall notify the Controller without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Data Breach affecting the Controller's Personal Data.

### 7.2 Content of Notification

The notification shall include, at minimum:

- A description of the nature of the Data Breach, including the categories and approximate number of Data Subjects and Personal Data records affected.

- The name and contact details of the Processor's contact point for further information.
- A description of the likely consequences of the Data Breach.
- A description of the measures taken or proposed to address the Data Breach, including measures to mitigate its possible adverse effects.

### 7.3 Assistance

The Processor shall cooperate with and assist the Controller in fulfilling the Controller's obligations under Articles 33 and 34 of the GDPR, including notification to the Supervisory Authority and communication to affected Data Subjects where required.

## 8. AUDIT RIGHTS

The Controller shall have the right to audit the Processor's compliance with this DPA. Audits shall be conducted with reasonable prior written notice (not less than thirty (30) days), during regular business hours, and in a manner that does not unreasonably disrupt the Processor's operations.

The Processor may satisfy the Controller's audit requirements by providing: (a) an independent third-party audit report or certification (e.g., SOC 2 Type II); (b) responses to the Controller's written audit questionnaire; or (c) access to relevant documentation and records demonstrating compliance.

## 9. LIABILITY

Each party's liability arising out of or in connection with this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement. Nothing in this DPA shall limit either party's liability for: (a) breaches of confidentiality obligations; (b) the Processor's indemnification obligations for processing in violation of the Controller's lawful instructions; or (c) either party's liability to the extent it cannot be limited under applicable data protection law.

## 10. TERM AND TERMINATION

### 10.1 Effective Date

This DPA shall become effective upon execution by both parties and shall remain in effect for the duration of the Agreement.

### 10.2 Survival

The obligations of the Processor under this DPA shall survive termination of the Agreement with respect to any Personal Data that remains in the Processor's possession or control.

### 10.3 Data Deletion

Upon termination of the Agreement, the Processor shall, at the Controller's election, delete or return all Personal Data within thirty (30) days. The Processor shall certify deletion in writing upon the Controller's request. Data may be retained beyond this period only where required by applicable law.

## 11. STANDARD CONTRACTUAL CLAUSES

To the extent that the Processing of Personal Data involves a transfer from the EEA, UK, or Switzerland to the United States, the Standard Contractual Clauses adopted by the European Commission in Implementing Decision (EU) 2021/914 are hereby incorporated by reference into this DPA.

- **Module Two** (Controller to Processor) shall apply.
- The **governing law** of the SCCs shall be the laws of the EU Member State where the Controller is established.
- The **competent supervisory authority** shall be the data protection authority of the EU Member State where the Controller is established.
- In the event of a conflict between this DPA and the SCCs, the SCCs shall prevail.

## 12. EXECUTION

By signing below, the parties acknowledge that they have read and agree to the terms of this Data Processing Agreement.

**CONTROLLER (Customer)**

Company: _____

Authorized Signatory: _____

Title: _____

Date: _____

Signature: _____

*The entity on whose behalf Personal Data is processed*

**PROCESSOR**

Company: Prismatic Solutions (UserDesk)

Authorized Signatory: _____

Title: _____

Date: _____

Signature: _____

*hello@getuserdesk.com | Pennsylvania, United States*