

Data Processing Agreement (Draft)

Data Processing Agreement

⚠ **DRAFT — requires legal review before use.** This document is a structured starting point for counsel to review, complete, and approve. It is not legal advice and must not be sent to any client before a qualified lawyer has reviewed it. Fields in [brackets] require verified details before publication.

Version 0.1 (draft) · Last updated: [DATE]

Parties

This Data Processing Agreement (“**DPA**”) is entered into between:

[**LEGAL ENTITY NAME**], a company registered under the laws of India, having its registered office at [REGISTERED ADDRESS] (“**Sypher**”, “**we**”, “**us**”),

and

[**CLIENT LEGAL NAME**], having its registered office at [CLIENT ADDRESS] (“**Client**”, “**you**”),

each a “**Party**” and together the “**Parties**.”

This DPA forms part of, and is incorporated by reference into, the Master Services Agreement between the Parties dated [MSA DATE] (the “**Agreement**”). In the event of any conflict between this DPA and the Agreement concerning the processing of personal data, this DPA prevails.

1. Definitions

Terms used in this DPA have the meanings given to them in the Digital Personal Data Protection Act, 2023 (“**DPDP Act**”) and its rules, including:

- “**Personal Data**” means any data about an individual who is identifiable by or in relation to such data.
- “**Data Principal**” means the individual to whom the personal data relates.
- “**Data Fiduciary**” means the entity that determines the purpose and means of processing personal data — in this engagement, the **Client**.
- “**Data Processor**” means the entity that processes personal data on behalf of a Data Fiduciary — in this engagement, **Sypher**.
- “**Processing**” means any operation performed on personal data, including collection, storage, use, disclosure, and erasure.
- “**Sub-processor**” means any third party engaged by Sypher to process personal data on Sypher’s behalf, in furtherance of this

DPA.

- **“Instance”** means the Client’s dedicated iSyph environment, comprising one or more Spaces configured under the Agreement.
-

2. Roles of the Parties

2.1. As between the Parties, the Client is the Data Fiduciary and Sypher is the Data Processor with respect to personal data processed within the Client’s Instance, including the content of messages, files, and the identities of individuals granted access by the Client (**“Client Personal Data”**).

2.2. Sypher processes Client Personal Data only:

(a) on the Client’s documented instructions, including those given through the Client’s own configuration of the platform (for example, granting or revoking a user’s access, or setting a Space’s retention period); and

(b) as necessary to provide the service described in the Agreement.

2.3. Sypher will not process Client Personal Data for its own purposes, and will not use Client Personal Data to train any machine-learning model, for advertising, or for any purpose other than providing the service to the Client.

2.4. Where Sypher determines that an instruction from the Client would result in a violation of applicable data-protection law, Sypher will notify the Client promptly and may suspend performance of that instruction pending resolution.

3. Nature and Purpose of Processing

3.1. **Subject matter:** the provision of a private, company-configured business communication platform.

3.2. **Duration:** for the term of the Agreement, and thereafter as set out in Section 9 (Deletion and Return).

3.3. **Nature and purpose:** hosting, transmitting, storing, and making available the Client’s business communications and associated account data, strictly as configured by the Client.

3.4. **Categories of Data Principals:** the Client’s employees, contractors, and other individuals to whom the Client grants access to the Instance.

3.5. **Categories of personal data processed,** as applicable to the Client’s configuration:

(a) **Account and access data** — name or alias, role, and the Spaces an individual has access to;

(b) **Conversation content** — messages and files exchanged within a Space, to the extent the Client has configured that Space to retain such content;

(c) **Client business-contact data** — names, phone numbers, and email addresses of the Client’s designated contacts, held as part of the Client’s account record rather than conversation content.

3.6. Sypher does not require, and the Client should not transmit through the platform, any special category of personal data (as recognised under applicable law) beyond what is ordinarily incidental to routine business communication, unless the Parties separately agree in writing on additional safeguards.

4. Client's Instructions and Configuration

4.1. The Client controls, through the platform's administrative tools, the following aspects of processing, each of which constitutes a documented instruction for the purposes of this DPA:

- (a) which individuals are granted or denied access to a Space;
- (b) the data-retention period applied to each Space, including an ephemeral (zero-retention) configuration under which no conversation content is stored;
- (c) which optional features (as described in the Agreement) are enabled for a Space;
- (d) requests to amend, suspend, or terminate the engagement.

4.2. Sypher will implement changes made under Section 4.1 without undue delay, and in the case of access revocation, promptly upon the Client's action.

5. Sub-processors

5.1. The Client authorises Sypher to engage the following categories of Sub-processor, each bound by written contract to data-protection obligations no less protective than those in this DPA:

- (a) **infrastructure hosting providers**, located in India, who host the servers on which the Instance runs, and who do not have access to the content of Client Personal Data in the ordinary course;
- (b) **transactional email delivery providers**, engaged solely to deliver operational emails (such as account notifications) on Sypher's behalf, who process only the message content and recipient address of that specific email.

5.2. A current, named list of Sub-processors is available to the Client on request.

5.3. Sypher will notify the Client of any intended change to its Sub-processors, and the Client may object on reasonable data-protection grounds within [NOTICE PERIOD — e.g. 30 days]. If the Parties cannot resolve the objection, either Party may treat this as a matter for escalation under the Agreement.

5.4. Sypher remains liable for the acts and omissions of its Sub-processors to the same extent as for its own acts and omissions under this DPA.

6. Location of Processing and Cross-Border Transfers

6.1. Client Personal Data is processed and stored on infrastructure located in India.

6.2. Sypher will not transfer Client Personal Data outside India in the ordinary course of providing the service. Should a transfer become necessary (for example, to comply with a legal obligation), Sypher will notify the Client in advance where legally permitted to do so, and will ensure any such transfer complies with the DPDP Act and applicable rules on cross-border transfer.

7. Security Measures

7.1. Sypher implements technical and organisational measures appropriate to the risk, including:

(a) access to the Client's Instance restricted to individuals the Client has authorised;

(b) role-based access controls for Sypher's own personnel, limiting administrative access to what is necessary to provide support;

(c) encryption of data in transit;

(d) logical separation of each Client's Instance and data from other clients;

(e) [FURTHER MEASURES — e.g. encryption at rest, access logging, penetration testing cadence — to be confirmed and completed by Sypher before this section is finalised].

7.2. Sypher will make available to the Client, on reasonable request, information necessary to demonstrate compliance with this Section 7, subject to reasonable confidentiality restrictions.

8. Personal Data Breach

8.1. Sypher will notify the Client without undue delay, and in any case within [NOTIFICATION WINDOW — to be confirmed, e.g. 72 hours] of becoming aware, of any Personal Data Breach affecting Client Personal Data.

8.2. Such notice will describe, to the extent then known: the nature of the breach; the categories and approximate number of Data Principals and records affected; the likely consequences; and the measures taken or proposed to address the breach.

8.3. Sypher will cooperate with the Client and provide reasonable assistance to enable the Client to comply with its own notification obligations under the DPDP Act, including notification to the Data Protection Board of India and to affected Data Principals where required.

8.4. Sypher will not disclose a Personal Data Breach involving Client Personal Data to any third party or public authority without the Client's prior consent, except as required by law, in which case Sypher will, where legally permitted, notify the Client before making such disclosure.

9. Assistance with Data Principal Rights

9.1. Where a Data Principal submits a request to the Client to exercise a right under the DPDP Act (including access, correction, or erasure), and the Client requires Sypher's assistance to respond, Sypher will provide reasonable technical assistance without undue delay.

9.2. Where a Data Principal contacts Sypher directly regarding Client Personal Data, Sypher will promptly redirect the request to the Client and will not itself act on the request except at the Client's direction, unless required by law.

10. Deletion and Return

10.1. On termination or expiry of the Agreement, Sypher will, at the Client's election made within [ELECTION PERIOD — e.g. 30 days] of termination, either:

(a) return Client Personal Data to the Client in a commonly usable format; or

(b) delete Client Personal Data,

except to the extent applicable law requires Sypher to retain it, in which case Sypher will continue to protect that data under the terms of this DPA for as long as it is retained.

10.2. Where deletion is elected or otherwise applies (including the routine expiry of a Space's configured retention period), such deletion is an irreversible removal of the data from Sypher's systems, not a logical or soft deletion that leaves the data recoverable.

10.3. For clarity, this Section does not apply to the record of the commercial engagement itself (the plan, features, and retention terms agreed between the Parties, and any amendments to them), which Sypher retains as a business record independent of this DPA for so long as necessary to evidence the Parties' engagement, including after termination.

11. Audit Rights

11.1. On reasonable prior written notice, and no more than [FREQUENCY — e.g. once per year] absent a reasonably suspected breach, the Client may request information reasonably necessary to verify Sypher's compliance with this DPA.

11.2. Sypher may satisfy such a request by providing a summary of its security practices, relevant policy documents, or, where the Client reasonably requires further verification, by permitting an audit conducted by an independent third party bound by confidentiality, at the Client's cost, during business hours, and without unreasonably disrupting Sypher's operations or other clients.

12. Liability

12.1. Each Party's liability arising under this DPA is subject to the limitations and exclusions of liability set out in the Agreement. [LIABILITY CROSS-REFERENCE / CARVE-OUTS — to be confirmed by counsel; data-protection obligations are sometimes carved out of a general liability cap and this needs a deliberate decision, not a default].

13. Term and Termination

13.1. This DPA takes effect on the effective date of the Agreement and remains in effect for as long as Sypher processes Client Personal Data under the Agreement.

13.2. Termination of the Agreement terminates this DPA, without prejudice to any rights or obligations that by their nature survive termination (including Sections 10, 11, and 12).

14. Governing Law

This DPA is governed by the laws of India, with jurisdiction in the courts of Pune City, Maharashtra, India, consistent with the Agreement.

Signatures

For [LEGAL ENTITY NAME]:

Name: _____ Title: _____ Date: _____

For [CLIENT LEGAL NAME]:

Name: _____ Title: _____ Date: _____