

Strata

Privacy Policy

Data controller: Cypher Capital Technology LLC

Effective date: 27 July 2026 **Last updated:** 27 July 2026

1. Introduction

This Privacy Policy explains how Cypher Capital Technology LLC (“CCT”, “we”, “us” or “our”) collects, uses, stores, shares and otherwise processes personal data in connection with Strata, an artificial-intelligence workplace assistant (the “Service”). CCT is the data controller responsible for the personal data processed through the Service.

Strata is currently provided to authorised personnel of Cypher Capital, Storm Group and their affiliated entities (the “Group”). Users access the Service using an organisational account and may connect the Service to third-party tools they are authorised to use. By accessing the Service and connecting these tools, you acknowledge the practices described in this Policy.

We process personal data in accordance with UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the “PDPL”). Where users or data subjects are located in the European Economic Area, the United Kingdom, Switzerland or the United States, the additional regional rights and disclosures in Section 12 also apply. We also comply with the requirements of the platforms we integrate with, including the Google API Services User Data Policy (Section 7).

2. Who we are and how to contact us

Controller: Cypher Capital Technology LLC

Privacy contact: legal@cyphercapital.com

3. Personal data we collect and process

We collect and process the following categories of personal data:

- **Account and identity data** — your name, work email address, organisation, role, profile image and the authentication identifiers and tokens used to sign you in and connect your tools.
- **Google Workspace data** — accessed through Google OAuth, and only after you grant permission: Gmail (message content and metadata, used to give you context, summarise correspondence and draft or send messages on your behalf); Google Calendar (events and attendees, used for meeting briefings); Google Drive (files you or your organisation authorise, which the Service may search, read and create); and Google Meet transcripts (recordings, transcripts and the derived notes, decisions and action items, including transcription generated using Google Gemini).
- **Connected third-party tools** — only those you choose to connect: Twenty CRM (contacts, companies, deals and pipeline data), Notion (workspace pages and content), and messaging platforms such as Telegram and Slack (messages and notifications you direct to or through the Service).
- **Usage and technical data** — the queries and instructions you submit, interaction logs, and device and connection information.

- **Memory data** — information the Service retains about you, derived from your prior interactions, to personalise and improve its responses to you.

We do not intentionally collect special categories of personal data through the Service. Please do not submit such data unless it is necessary and lawful to do so.

4. How we use personal data and our legal bases

We use personal data to provide the Service's features (meeting intelligence and search, tracking of action items and decisions, calendar and meeting preparation, drafting and sending communications at your direction, CRM and deal tracking, reporting, and creating or updating documents and records); to personalise the Service to you (including through the memory feature); to operate, secure, maintain and improve the Service; and to comply with our legal and regulatory obligations.

Legal bases. Under Article 4 of the PDPL we rely on your consent and on the processing being necessary for the arrangement under which the Service is provided. For data subjects to whom the GDPR or UK GDPR applies, we rely on the following legal bases:

Purpose	Legal basis (GDPR / UK GDPR)
Providing and operating the Service to you and your organisation	Performance of a contract; legitimate interests
Personalisation, security, maintenance and improvement	Legitimate interests (running and securing the Service)
Connecting Google and third-party tools and processing their data	Consent (granted via OAuth and the connection settings)
Legal, regulatory and compliance obligations	Compliance with a legal obligation

Automated writes and actions — for example, creating or updating records, or sending messages — require your explicit approval before they are executed.

5. Cookies and analytics

The Service uses cookies and similar technologies that are strictly necessary to authenticate you and maintain your session. We do not use cookies for third-party advertising.

6. How we share personal data — sub-processors

We share personal data with the service providers and sub-processors that host and operate the Service and provide its integrated functionality. Our current sub-processors are:

Recipient	Purpose	Primary location
Cloud hosting and infrastructure provider	Hosting and infrastructure	United States
Google LLC (incl. Gemini)	Workspace integration; meeting transcription and notes	United States
Anthropic (Claude)	Language processing that generates the Service's responses	United States

Recipient	Purpose	Primary location
Twenty	CRM / deal data integration	United States
Notion Labs	Workspace pages integration	United States
Telegram; Slack	Messaging integration (where connected)	United Arab Emirates (Telegram); United States (Slack)

An up-to-date list of sub-processors is maintained at strata.cyphercapital.com/subprocessors. We also share personal data with other authorised users within your organisation (subject to the visibility settings available to you); with professional advisers, regulators and authorities where required or permitted by law; and with a successor entity in connection with a merger, acquisition or sale of assets. We do not sell personal data, and we do not share personal data for cross-context behavioural advertising.

7. Google API Services — Limited Use

Strata's access to, and use, storage and sharing of, information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements. In particular:

- we use Google user data only to provide and improve the user-facing features of the Service that are prominent in the Service's user interface;
- we do not transfer Google user data except as necessary to provide or improve those features (and then only with your consent), for security purposes, to comply with applicable law, or as part of a merger, acquisition or sale of assets;
- we do not use Google user data for serving advertising, and we do not sell Google user data;
- we do not use Google user data to develop, improve or train generalised or non-personalised artificial-intelligence or machine-learning models; and
- we do not allow humans to read your Google user data unless: (i) we have first obtained your affirmative agreement to view specific messages, files or other data; (ii) it is necessary for security purposes or to comply with applicable law; or (iii) the data has been aggregated and anonymised.

Restricted-scope Google data, such as Gmail data, is used solely to deliver the Service's features to you and is handled in accordance with these commitments.

8. Artificial-intelligence processing and our no-training commitment

The Service relies on third-party artificial-intelligence providers to deliver its features, including Google (Gemini) for meeting transcription and note generation and Anthropic (Claude) for the language processing that generates the Service's responses. When you submit a query, or the Service prepares an output, relevant content is transmitted to these providers solely to generate the response or feature you have requested.

We do not use your content — including your Google user data and your meeting content — to develop, train or improve generalised or non-personalised artificial-intelligence or machine-learning models, we do not train our own models on your content (including on de-identified content), and we contractually prohibit our artificial-intelligence providers from using your content to train or improve their own models.

Automated writes and actions require your explicit approval before they are executed.

9. International data transfers

The Service and certain of our sub-processors operate outside the UAE, including in the United States. Where we transfer personal data outside the UAE, we do so in accordance with the PDPL, relying on your consent and/or the other bases permitted under the PDPL, with contractual and organisational safeguards.

Where we transfer personal data from the European Economic Area, the United Kingdom or Switzerland to a country that has not received an adequacy decision, we rely on appropriate safeguards, principally the European Commission's Standard Contractual Clauses (together with the UK International Data Transfer Addendum and the Swiss addendum, as applicable), supported by additional measures where required.

10. Data retention

We retain personal data only for as long as necessary for the purposes described in this Policy or as required by law. Indicative retention periods:

Category	Retention
Account and profile data	For the duration of your authorisation, then deleted within 30 days of account closure
Google Workspace data	Only while your Google account is connected; access ceases and cached data is purged on revocation
Meeting transcripts, notes and action items	No longer than 24 months, unless you delete them sooner
Usage and technical logs	Up to 12 months
Memory data	Until you clear it, or when your account is closed

You may disconnect integrations or revoke the Service's access to your Google account at any time through your Google Account settings or the Service's connection settings; on revocation, the Service will cease further access to the relevant data.

11. Security

We implement appropriate technical and organisational measures designed to protect personal data against unauthorised access, disclosure, alteration and loss, including access controls, encryption of data in transit and at rest, and approval gating of automated actions. We maintain procedures to address personal-data breaches and will notify affected parties and regulators where required by law. No system can be guaranteed to be completely secure.

12. Your rights

12.1 All users (UAE PDPL)

Subject to the PDPL, you have the right to: be informed about and access your personal data (Article 13); receive it in a structured, machine-readable format (Article 14); request correction or erasure (Article 15); request restriction of, or that we stop, processing (Articles 16 and 17), including objecting to direct marketing; object to decisions based solely on automated processing that produce legal consequences (Article 18); and withdraw consent at any time.

To exercise these rights, contact us at legal@cyphercapital.com. You may also lodge a complaint with the UAE Data Office.

12.2 EEA, UK and Switzerland (GDPR / UK GDPR / FADP)

If you are in the EEA, the UK or Switzerland, you have the rights to access; rectification; erasure; restriction of processing; data portability; to object to processing based on our legitimate interests and to direct marketing; and not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. Where we rely on consent, you may withdraw it at any time without affecting prior processing. We aim to respond within one month. You also have the right to lodge a complaint with your local supervisory authority. The legal bases for our processing are set out in Section 4 and our transfer safeguards in Section 9.

12.3 United States (California and other states)

We do not “sell” your personal information, and we do not “share” it for cross-context behavioural advertising, as those terms are defined under the California Consumer Privacy Act (as amended) and comparable state laws. The categories of personal information we process are described in Section 3 (identifiers, professional or employment-related information, commercial information, internet or electronic activity, and inferences). Subject to applicable law, you have the rights to know/access, delete, and correct your personal information; to opt out of sale, sharing and targeted advertising; to non-discrimination for exercising your rights; and to appeal a decision. You may use an authorised agent. To exercise these rights, contact us at legal@cyphercapital.com.

13. Children

The Service is intended for use by authorised business users and is not directed to children.

14. Changes to this Policy

We may update this Policy from time to time. If we change the way we use Google user data, we will notify affected users and obtain their consent to the updated Policy before using Google user data in the new way.

15. Governing law

This Policy, and any matter arising out of or in connection with it, is governed by the laws of the United Arab Emirates as applied in the Emirate of Dubai. The regional provisions in Section 12 grant additional statutory rights to data subjects in the relevant jurisdictions and do not change the governing law of this Policy.