Zoom Regional Infrastructure
FACT SHEET

I. Introduction

As part of our commitment to customer satisfaction, Zoom's growth strategy is dedicated to addressing evolving customer needs, corporate policies, contractual obligations, and global regulatory trends: this requires increased options for local data storage, which refers to the processing and storing of data in a specific geographical location.

Zoom lets customers localize personal data Zoom processes to deliver the services. This applies to certain products, such as, but not limited to, Meetings, Webinars and Phone. Some exceptions apply, including as required by applicable law, for trust and safety purposes, and to provide service notifications and enable the services, as described below.

II. Zoom Regional Infrastructure

For international customers who do not wish to transfer personal data (Content, Account, and Diagnostic Data) outside their region, Zoom offers dedicated infrastructure (**Zoom Regional Infrastructure**) to house Education and Enterprise customers' accounts in specific geographic locations (see Zoom Regional Infrastructure Offerings). For more information on the categories of personal data, please visit Zoom's Privacy Trust Center.

Zoom provides customers hosted in Zoom Regional Infrastructure with the ability to process and store data in-region, and only transfer personal data outside of the region in accordance with jurisdictional regulations. Personal data is not transferred outside of or accessed from outside Zoom Regional Infrastructure unless previously agreed upon with the customer, or to the extent that certain exceptions apply (see Global Service Exceptions below).

III. Zoom Regional Infrastructure Cloud Technologies

For customers hosted within Zoom Regional Infrastructure, customers will connect to data centers located in the region. However, they can connect to any number of data centers outside the region based on their geolocation (if they travel abroad or accept participants from different geolocations, for example), their account setup, and by interacting with external accounts not hosted in Zoom Regional Infrastructure.

Customers can choose to be hosted in a local data center in one of the regions listed in the Zoom Regional Infrastructure Offerings (see below). Customers may also choose to store a

subset of data locally on their own devices or in their local data center. Zoom Phone and Zoom Contact Center customers hosted on Zoom Regional Infrastructure can choose to connect their on-net calls (non-PSTN) through in-country SIP zones. Zoom Phone and Zoom Contact Center recordings, voicemail and voicemail transcripts, and other content will be stored in the region.

For supported AI Companion features, Zoom-hosted models are made available to regionally hosted customers. Zoom-hosted Models Only means that customer data will not be sent outside of Zoom's cloud platform to third-party models. You can read about security and privacy features in our AI Companion whitepaper.

IV. Zoom Regional Infrastructure Offerings

Zoom Regional Infrastructure is available in the following regions:

1. Australia
2. Canada
3. European Union
4. India
5. Saudi Arabia
6. Singapore
7. United Kingdom

NOTE: Not all products may be available. Please reach out to your Zoom representative for additional information.

V. Zoom Regional Infrastructure Digital Controls

Access Controls

Organizational Controls. Zoom's access to customer data is role-based and restricted based on least privilege, in accordance with Zoom's access control policies and standards. Controls are in place to prevent Zoom employees from accessing customer content, including meeting, webinar, chat, or email content (specifically, audio, video, files, in-meeting whiteboards, messaging, SMS, or email content), or any content generated or shared as part of other collaborative features, unless authorized by the account owner hosting the Zoom product or service where the customer content was generated, or as required for legal, safety, or security reasons. Zoom's access to customer data and content is logged and monitored for suspicious activity or unauthorized access.

Customer Support. For more sensitive customer data, controls are in place that require an organization's approval for Zoom to access the data to troubleshoot issues, including (but not limited to):

- Recordings
- Chat history
- Whiteboards

Access is also time bounded so Zoom does not have persistent access to this data.

End-to-End Encryption

Additional security controls exist for customers to secure their meetings. Customers that are interested in additional encryption features can enable E2EE for their meetings. However, they should be aware of the prerequisites and limitations.

Team Chat has a similar advanced encryption option. A key limitation to note is that messages may not be able to be decrypted if participants are not online at the same time since keys are generated on the users' devices and exchanged with each other. Before enabling this feature, customers should be aware of issues that may arise when trying to decrypt messages.

Account admins can also enable E2EE for one-on-one Zoom Phone calls with certain limitations. Zoom Phone E2EE is available when the caller and callee are part of the same Zoom account, are joining from the Zoom desktop or mobile client, and automatic call recording is disabled or paused during the call. E2EE is not available for web client and PSTN calls, Zoom Contact Center, and Zoom Virtual Agent at this time.

Zoom Customer Managed Key

Zoom Customer Managed Key (CMK) allows organizations to provide and manage their own encryption keys for certain data stored in Zoom's cloud.

Zoom supports Amazon Key Management Service (KMS), Oracle OCI Vault, Azure Key Vault and Thales CipherTrust via Amazon KMS External Key Store (XKS). This allows organizations to bring their own keys and manage them within their cloud provider.

Zoom Customer Managed Key supports various data in Zoom such as:

- Meeting/Webinar recordings (including transcripts, summaries and in-meeting chat, but does not currently support search index)
- Phone voicemails and recordings
- Team Chat messages
- Whiteboards and Clips
- Calendar access tokens for Zoom Rooms
- User calendar and Microsoft Teams access tokens
- Contact Center voice and video recordings and transcripts, voicemail and voicemail transcripts, and messaging transcripts

Additional details are available in the Zoom Customer Managed Key whitepaper.

VI. Global Service Exceptions

Personal data of customers hosted in Zoom Regional Infrastructure is not transferred outside of the region unless previously agreed upon with the customer. Some exceptions apply, including as required for legal, safety, security, support, billing, to provide service notifications, and to enable the services.

Safety & Security

Customer personal data may be processed and stored outside the region for safety and security purposes.

As an example, customer personal data may be shared with U.S. teams in individual cases, such as those requiring review by Zoom's Trust & Safety team (for example, if Zoom received a complaint about a user, or its security systems flag a user), and under the following conditions:

- When the personal data does not contain direct identifiers like email, instead use pseudonymised identifiers like UUID, or CIDs, or
- When the data is necessary for abuse and fraud prevention.

Customer personal data may be accessed and stored outside of the region by Trust & Safety Agents. Trust & Safety Agents are:

- Subject to strict role-based access controls, and
- Access is logged and monitored.

Support

Our global support operates 24/7 through a follow-the-sun model with strategically positioned international personnel. Support agents operate from multiple countries and utilize U.S.-based platforms for ticket management.

Analytics

Zoom has a legitimate business purpose for product usage analytics and customer relationship management. To learn more please refer to the Zoom Privacy Statement.

Billing

Account Holder Business Data may be transferred outside of the region for billing purposes.

Service Notifications

Zoom uses U.S.-based services to send service notifications, such as “Forgot My Password”, “User has joined your meeting”, and Data Subject Rights Request notifications. Users cannot fully opt-out of this processing and transfer of customer data because some communications are necessary to provide the Service.

Global Platform Operations

Zoom is a global communications platform and users rely on Zoom to interact with each other worldwide. For instance, as part of pre-meeting activities, Zoom processes a limited amount of personal data critical for operations that are required to operate Zoom (such as Account ID, User ID and Meeting ID/PMI). Examples of these types of operations include securing the platform by ensuring meetings and users are uniquely identifiable, allowing users to log into their account and interacting with all Zoom users worldwide while ensuring the services adhere to the meeting host’s settings. These operations are hosted in the U.S.

Additional services are available worldwide to enable globally distributed participants to connect to each other and improve quality of service. This includes local dial-in numbers and geographically distributed data centers which can be enabled on an account, group, or user level for their hosted meetings. You can find details in this Help Article.

APIs & Marketplace Apps

APIs and Marketplace apps (including both custom and third-party integrations) are disabled by default. An administrator can choose to allow access to both custom and third-party apps. If users install such an app, they can give access to their Zoom account via the API. Zoom Marketplace apps and APIs may store and process data in the US. Zoom does not own or manage the apps developed by third-party app developers (including both custom and third-party apps). Please refer to each individual app for more information specific to using the app, installation requirements, privacy notice, and support.

VII. Our Ongoing Commitment

We have a strong commitment to respect customer and regulatory expectations related to data privacy. Working with our partners, we continue to refine, adapt, and expand our strategy and platform to deliver for our customers around the world.

This Zoom Regional Infrastructure Fact Sheet specifies our Privacy Practices, does not create additional rights or remedies, and should not be construed as a binding agreement.

Additional information can be found at https://explore.zoom.us/en/gdpr/.

Please get in touch with us at privacy@zoom.us with any questions or comments.