Zoom EU 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 EU Infrastructure

For customers based in the European Union (**EU**) who do not wish to transfer personal data (Content, Account, Diagnostic, Support and the restricted access Website Data) to the U.S., Zoom offers dedicated infrastructure (the **Zoom EU Infrastructure**) to house EU Education and Enterprise customers' accounts.

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

III. Zoom EU Infrastructure Cloud Technologies

For customers hosted within the Zoom EU Infrastructure, Zoom uses a mix of cloud technologies and its own colocated data centers to deliver its services. Normally, customers hosted in the Zoom EU Infrastructure will connect to Amazon Web Services (AWS) data centers and colocations in the EU. The AWS data centers and colocations are located in the EU but they can connect to any number of colocation sites (data centers) or clouds, 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 the Zoom EU Infrastructure.

Customers hosted within the Zoom EU Infrastructure can choose data center regions for all the Zoom products listed in the Zoom EU 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 EU Infrastructure can choose to connect their on-net calls (non-PSTN) through in-region SIP zones. Zoom Phone and Zoom Contact Center recordings, voicemail and voicemail transcripts, and other content will be stored in the EU.

For AI Companion features, both Zoom-hosted models and Anthropic models are made available to EU hosted customers. Anthropic models are made available using Amazon Bedrock, which is a fully managed service provided through Zoom's existing cloud services provider AWS. Any customer content processed through Amazon Bedrock is encrypted and stored at rest in the EU. Inputs and outputs are not shared with any model providers. Further, Amazon confirms that Bedrock can be used in compliance with the General Data Protection Regulation (GDPR). Customers also have the option to instead use Zoom-hosted Models Only, which means that customer data will not be sent outside of Zoom's cloud platform to third-party models. We are also committed to not use any customer audio, video, chat, screen sharing, attachments, or other communications-like customer content (such as poll results, whiteboard, and reactions) to train Zoom's or its third-party artificial intelligence models. You can read more about our approach and when additional features will be available to EU hosted customers in our whitepaper about the security and privacy features in Zoom AI Companion.

IV. Zoom EU Infrastructure Offerings

1. Meetings
2. Webinar
3. Team Chat
4. Phone
5. Contact Center
6. Whiteboard
7. Notes
8. Events
9. Sessions
10. Revenue Accelerator
11. Rooms
12. Workspace Reservations

13. Digital Signage
14. Visitor Management
15. AI Companion
16. Docs
17. Clips
18. Zoom Mail & Calendar
19. Scheduler
20. Zoom Virtual Agent
21. Workforce Management

V. Zoom EU Infrastructure Digital Controls

Access Controls

Organizational Controls. Zoom's access to customer data and content 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:

- 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 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 EU customers hosted in the regional Zoom EU Infrastructure is not transferred outside of the regional Zoom EU Infrastructure unless previously agreed upon with the

customer. Some exceptions apply, including as required by applicable law, for trust and safety purposes, and to provide service notifications and enable the services.

Trust & Safety Data

Customer personal data may be shared with U.S. teams in individual cases and exceptional circumstances, 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 Europe by Trust and Safety Agents. Trust & Safety Agents are:

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

Support Agent Access

Upon request, Zoom offers EU hosted customers the possibility to have all of their Support Data processed within the EU. If an EU Infrastructure based customer requires support outside of regular working hours in the EU, the customer can consent on a case-by-case basis to the specific transfer of personal data to a helpdesk outside of the EU. Zoom gives customers an option to provide specific consent if they want to authorize Zoom to transfer incidental support requests to its support staff internationally.

Analytics

Zoom has a legitimate business purpose for product usage analytics and customer relationship management. Zoom can use non-sensitive and aggregated user-level data, along with Account ID, for these legitimate purposes. The Account ID is not considered personal data for Enterprise or Education customers.

Diagnostic Data will be de-identified before being sent to Zoom's U.S. based teams for analysis. Zoom combines multiple data points into larger datasets while stripping away identifying information in three different ways — in-region federated queries, global exceptions, and cohort grouping. This is done to protect the privacy of individuals while retaining the ability to derive insights from the data as a whole on an account level.

Billing

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

Service Notifications

Zoom uses US-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 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 Europe and 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 in Europe and around the world.

This Zoom EU 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.