Privacy Data Sheet
Zoom Meetings, Chat and Webinar

I. Introduction

This Privacy Data Sheet describes the processing of information from or about an identified or identifiable person ("Personal Data") by Zoom's Meetings, Chat, and Video Webinar product (collectively, "the Services"). It applies to the Services available to organisations through the purchase of a Zoom account ("Customers") and individuals that host or participate in the Services ("end users"). This Privacy Data Sheet does not apply to the Personal Data Zoom collects on behalf of Zoom accounts held by a natural person ("consumers''). Nor does this Privacy Data Sheet apply to Zoom for Government, Zoom Phone, Zoom Events or Zoom Apps.

This Privacy Data Sheet specifies our Privacy Statement in describing the Personal Data Zoom processes to provide the Services to our Customers and other data protection matters such as international data transfers and data location. It does not create additional rights or remedies and should not be construed as a binding agreement.

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

II. Data Protection Roles and Processing Purposes

Zoom is the data processor (as defined in the European Union's General Data Protection Regulation or "GDPR") for all Personal Data processed in delivery of the Services unless explicitly stated as an exception below.

Zoom Customers—such as employers or schools—control the processing of that Personal Data and related Zoom account settings. Zoom Customers can access the Personal Data described below and use it subject to their own policies and procedures.

Why Zoom Processes Personal Data

Zoom processes Personal Data as a processor only for the following purposes:

- To provide and update the Zoom Services as licensed, configured, and used by our Customers and their users, including through Customer's use of Zoom settings, administrator controls, or other Service functionality;
- To secure and protect the Zoom Services;
- To resolve issues, bugs, and errors;
- To provide Customers with support upon request, including applying knowledge gained from individual customer support requests to benefit all Zoom customers, but only to the extent such knowledge is anonymized; and
- To perform instructions explicitly authorised by the Customer in a written document.

Zoom processes Personal Data obtained through the delivery of the Services as controller (as defined in the GDPR) **only** for the following exhaustive list of purposes:

- To manage Customer business accounts, for example, billing, marketing communication with procurement or sales officials), and related Customer correspondence (e.g., communication about necessary updates);
- To comply with and resolve legal obligations, including responding to Data Subject Requests for Personal Data processed by Zoom as controller (for example, website data), fiscal requirements, agreements and disputes; and
- For abuse detection, prevention and protection (such as automatic scanning for matches with identifiers of known Child Sexual Abuse Material ("CSAM"), virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and actions not permitted under Zoom's Community Standards (also known as an acceptable use policy).

Zoom processes pseudonymised Personal Data or aggregated data as a controller for:

- improving and optimising the performance and core functionalities of accessibility, privacy, security, and the IT infrastructure efficiency of the Services, including zoom.us, explore.zoom.us, and support.zoom.us;
- internal reporting, financial reporting, revenue planning, capacity planning, and forecast modelling (including product strategy); and
- receiving and using feedback for Zoom's overall service improvement.

Whether acting as a processor or controller, Zoom processes Personal Data only where adequate, relevant, and where such processing is not excessive in relation to the specified purposes.

III. Personal Data Zoom Processes to deliver the Services

Zoom processes the following categories of Personal Data: Customer Content Data, Diagnostic Data, Account Data (end users), Account Holder Data, Support Data, Website Data, and Feedback Data.

Customer Content Data

Customer Content Data is information provided by the Customer through use of the Services including all data the Customer chooses to record or share during a meeting or webinar, including cloud recordings, meeting transcripts, chat transcripts (in-meeting & persistent), and files that are exchanged during a meeting or in the persistent chat channel. Additional detail on Customer Content Data follows:

Meeting and Webinar Communication Content. This includes:

- Video, audio, whiteboard, captions, and presentations
- In-meeting Questions & Answers, polls, and survey information
- Closed captioning (Live Transcription)

Chat Messages. 1:1 in-meeting and group chat messages that are not transferred to a permanent chat channel.

Customer Initiated cloud recordings. This includes the following recordings (if such recording is permitted by the Customer account administrator and the functionality is utilized by a meeting host or participant):

- Video recording of video, audio, whiteboard, captions, and presentations
- Audio recording
- Text file document of all in meeting group chats
- Audio transcript text file
- In-meeting Questions & Answers, polls, and survey information
- Closed captioning transcripts

Meeting and Webinar Participant Information. This includes:

- Registered participant name and contact details, and any data Customer optionally collects in conjunction with registration such as an email address
- Status of participant (as Host, as participants in a chat, or as attendees)
- Room Names (if used)
- User categorizations (if used)
- Tracking fields such as department or group (if used)
- Scheduled time for a meeting
- Topic names

Stored Chat Information. This is data at rest (in storage) and includes:

- Chat messages
- Files exchanged via Chat
- Images exchanged via Chat
- Videos exchanged via Chat
- Chat channel title
- Whiteboard annotations

Address book Information. This includes optional contact information made available through Customer controlled integrations (e.g., Outlook).

Calendar Information. This includes optional calendar information made available through Customer controlled integrations (e.g., Outlook, Google).

Diagnostic Data

Diagnostic Data includes all data automatically generated or collected by Zoom about the use of Zoom's meeting and webinar product. ***Diagnostic Data does not include a Zoom user's name, email address, or Customer Content Data.*** Diagnostic Data comprises three categories of data, Meeting Metadata, Telemetry Data, and Other Service Generated Data.

Meeting Metadata

Meeting Metadata are metrics about Service usage, including when and how meetings took place. This category includes:

- Event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID),
- userID and meeting ID,
- Meeting session information, including frequency, average and actual duration, quantity, quality, network activity, and network connectivity,
- Number of meetings,
- Number of screen-sharing and non-screen-sharing sessions,
- Number of participants
- Meeting host information
- Hostname
- Meeting site URL
- Meeting start/end time
- Join method
- Performance, troubleshooting, and diagnostics information.

Telemetry Data

Telemetry Data is information sent to Zoom from the Zoom client software running on an end user's device. It is information about how Zoom is used or performing (e.g., product usage and system configuration). ***Telemetry Data does not include Customer Content, or information about other users, meeting names, or other user-supplied values such as profile names.***

Zoom collects Telemetry Data following a similar structure: a few fields describe the client and the operating system, the type- and subtype of the event, the location in the app where the event occurred, a timestamp, and some pseudonymous identifiers, including a UUID, userID and meeting_id.

Telemetry Data Fields Common for All Events

This data is collected for **all** Events on the Zoom Client.

- Event time
- Client type

- Event location
- Event
- Subevent
- UUID
- Client version
- UserID
- Client OS
- Meeting ID

Telemetry Event Types and Subevent Types

Please visit Zoom's Telemetry Events Support page for more detailed documentation on event types and subevent types. Please note that the list of Telemetry Events is dynamic and will be updated. Zoom maintains privacy and security processes for approving the contents and purpose of proposed new events before such events can be added.

Other Service Generated Data

Diagnostic Data that is Other Service Generated Data is information that Zoom uses to provide a service requested by the end-user or Customer, such as providing spam warning notices or push notifications.

Other Service Generated Data also includes a Zoom persistent unique identifier that Zoom's Trust and Safety Team produces by combining other data elements including IP address, data center, PC name, microphone, speaker, camera, domain, hard disc ID, network type, operating system type and version, and client version. Zoom uses this data to identify and block bad actors that threaten the security and integrity of Zoom Services. This data is accessible only by Zoom employees who need to know and are subject to appropriate technical and organizational measures.

Account Data (end-user)

This is information associated with end-users of a Zoom Enterprise or Education account. Depending on how the account administrator has configured the Zoom Enterprise or Education account, this information includes:

- Zoom unique user ID,
- Social media login (optional),
- profile picture (optional),
- display name, and
- Customer authentication data unless Single Sign On ("SSO") is used.

Account Holder Business Data

This is information associated with the individual(s) who are the billing and or sales

contact for a Zoom Enterprise or Education account, including:

- name
- address
- phone number
- email address
- billing and payment information, and
- data related to the Customer's account, such as subscription plan and selected controls.

Support Data

Support data is information provided to Zoom by a Customer in connection with support activities such as support bot messages, chats, and phone calls (including recordings of those calls) and Service support tickets. The business contacts for a Zoom Education and Enterprise account or the account administrators can submit online support requests. The request can include attachments, such as screenshots. Such screenshots may include Customer Content Data or Diagnostic Data.

As controller, Zoom Customers instruct Zoom to process Support Data to provide the requested support, which includes applying knowledge gained from individual customer support requests to benefit all Zoom customers but only to the extent such knowledge is anonymized.

Website Data

Website Data is information about when and how people visit and interact with Zoom's public-facing websites, including information about what pages are accessed, interactions with the website features, and whether they signed up for a Zoom offering. Zoom's Website Data includes:

- cookies as determined by the end user's jurisdictions and choices (the Zoom Cookie Statement)
- Internet protocol (IP) address
- Browser type
- Internet service provider (ISP)
- Referrer URL
- Exit pages, the files viewed on our website (e.g., HTML pages, graphics, etc.),
- Operating system
- Date/time stamp
- Approximate location (e.g., nearest city or town, derived from IP address)

EU Based End Users and Cookies

Zoom sets only strictly necessary cookies on our public websites by default for EU-based end users. Please see our Cookie Statement for more information on your choices.

Feedback Data

Feedback data is information about end users' satisfaction with Zoom Services. There are two types of Feedback Data: (1) post-meeting assessments and (2) in-meeting surveys. Post-meeting assessments are a module that appears immediately after a Zoom meeting or webinar and asks the end-user to rate their Zoom experience by selecting a thumbs up or thumbs down icon. Depending on how Customer configures their Zoom account, they may enable the post-meeting assessment to collect only the thumbs up/thumbs down info, or Customers may seek additional information by presenting a free text submission box. The post-meeting assessment is not enabled by default.

An in-meeting survey is a tool deployed by Zoom to establish a Zoom Net Provider Score ("NPS"). This survey tool is off by default for EU based end users. All other end users can disable it by selecting only Strictly Necessary Cookies in Zoom's Cookie Management Tool which can be found by selecting “Cookies” in the footer of Zoom’s website pages.

IV. International Data Transfers

Zoom strives to transfer Personal Data per applicable data protection law. For example, where we transfer Personal Data outside the European Economic Area ("EEA"), Switzerland, or the UK, we do so based on the appropriate EU Standard Contractual Clauses (“SCCs”) with additional safeguards in place, as appropriate, so that the Personal Data is protected to the required standard.

The SCCs, Data Transfer Impact Assessments, and Schrems II

On 16 July 2020, the Court of Justice of the European Union (“CJEU”) ruled in the case of the Irish Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) ("Schrems II"). The ruling invalidated the EU-US Privacy Shield Framework as a lawful means to transfer Personal Data from the EEA to the US.

More importantly, however, the CJEU affirmed that the SCCs remain a valid Personal Data transfer mechanism – subject to a new requirement. To rely on the SCCs following Schrems II, data exporters must conduct a Data Transfer Impact Assessment (“DTIA”) to assess the risks of individual transfers and adopt any supplementary measures needed to bring the data protection level to the EU standard of essential equivalence.

We’ve prepared this template DTIA to help our Customers perform a risk assessment pursuant to the Schrems II decision. Please note that the DTIA does not form a part of any Zoom contractual document or agreement. It is provided solely as a source of information and reflects Zoom's understanding of complex legal issues. You should make your own determinations and, if necessary, seek independent legal advice.

Zoom also shares Personal Data we collect as a data processor with subprocessors, including members of the Zoom Group. You can find can find further information about these recipients in Section VII. Subprocessors in this Privacy Data Sheet.

V. *Government Requests to access Personal Data*

Zoom is committed to protecting our Customers and end users' privacy and only produces user data to governments in response to valid and lawful requests following our Government Requests Guide and relevant legal policies. Please see this blog post for further information on how we respond to government requests. To access our latest Transparency Report, visit our Trust Center and select the Government Requests Transparency Report icon.

VI. *Data location: Data in transit & Data at rest*

Data in transit

Data in transit, or data in motion, is data actively moving from one location to another, such as across the internet or through a private network. Zoom delivers the Services through its global network of collocated data centres and public cloud data centres, which are predominately operated through Amazon Web Services ("AWS"). The Services are designed to work so that any information entering the Zoom ecosystem is routed through the data centre nearest the user sending or receiving the data.

Zoom lets Customers make choices about the data centers that process Customer data in transit. Account-holders and the administrators of paid accounts can customize which data center regions they use for hosting their real-time meeting and webinar data in transit. You can opt-in or opt-out of certain data center regions for data in transit. Your default region, which is the region where your account was provisioned, will be locked. See this Help Article.

Data at rest

Customer Content, Account Data, and Operation Data are stored in the US by default. Customers may choose the storage location for some of their Customer Content for their account. You can find details in this Help Article.

Keep in mind this storage selection location does NOT include Account Data and Diagnostic Data, which will still be stored in the US. Only Account holders, account administrators, or those with the customer account profile privilege will be able to change this setting. Data at rest is encrypted using AES-256 GCM, with keys managed by a cloud-based key management system.

VII. Subprocessors

When Zoom hires suppliers to process Personal Data to provide certain aspects of the Services, these suppliers are "subprocessors" (following GDPR terminology) listed on Zoom's Subprocessor webpage.

Zoom's process for contracting with third-party subprocessors

Zoom requires its subprocessors to process Personal Data in accordance with applicable data protection law and to satisfy equivalent obligations as those required of Zoom as a data processor and outlined in Zoom's Data Processing Agreement ("DPA"), including but not limited to the requirements to:

- process Personal Data following the controller's (i.e., Customer's) documented instructions (as communicated in writing to the relevant subprocessor by Zoom);
- in connection with the subprocessing activities, use only personnel who are reliable and subject to a contractually binding obligation to observe data privacy and security, to the extent applicable, under applicable data protection laws;
- promptly inform Zoom about any security breach; and
- cooperate with Zoom to address requests from data controllers, data subjects, or data protection authorities, as applicable.

Zoom Group Subprocessors

Zoom Video Communications, Inc. owns and controls several global affiliates that form the Zoom Group. All parties of the Zoom Group have entered the appropriate data transfer agreement that sets out the data protection requirements and incorporates the appropriate EU Standard Contractual Clauses ("SCCs"). Zoom's subprocessor page lists the Zoom Group affiliates.

VIII. Security (Technical & Organizational Measures): Certifications & Compliance

Zoom implements and uses appropriate technical and organizational measures to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction, taking into account the risks involved in the processing and the nature of the Personal Data. The following third-party validations underpin Zoom's commitment to data protection:

- Annual SSAE-18 SOC 2 (Type II) Attestation
- FedRAMP (Moderate), for Zoom for Government
- Alignment with the UK National Cyber Security Centre's Cloud Security Principles

- ISO 27001 Certification
- SOC 2 + HITRUST Attestation
- CSA STAR Level 2 Attestation

Please see our Trust Center's Security Pages for more information on how Zoom works to secure your data and protect your privacy.