Privacy Data Sheet
Zoom Phone

I. Introduction

This Privacy Data Sheet describes the processing of personal data, which is information from or about an identified or identifiable person ("Personal Data") by the wholly owned subsidiary of Zoom Video Communications ("Zoom") that is the provider of the Zoom Phone Service ("Services"). Zoom Phone is a cloud-based phone service (available for our customers, companies and their employees and users (collectively, "Customers", "you" or "your"). Specifically, the Services include the following:

- **Telephony.** Zoom Phone is a cloud-based phone service that uses voice over internet protocol (VoIP) to provide two-way voice calling and private branch exchange (PBX) functionality . It is offered through a unified app for phone, video, meetings and chat, and provides internal business VoIP and PBX functionality. Zoom Phone enables on-net calls and provides access to a range of Zoom call management features and functions. Customers can add telephony services in two ways:
    - **Public Switched Telephone Network Communications (PSTN) Access.** Customers can make and receive PSTN calls and be assigned a direct inward dialing phone number (DID) via a Zoom Phone Calling Plan. In order to place PSTN calls, Zoom uses underlying providers to establish access to the PSTN .
    - **Bring Your Own Carrier (BYOC).** The BYOC feature allows customers to use the telecommunications provider of their choice to provide PSTN access and inward DID numbers. This in turn enables customers to (i) have PSTN capability in regions where Zoom does not offer PSTN Access; (ii) maintain relationships with currently deployed carriers; and/or (iii) configure deployments for flexibility and redundancy. Simply put, BYOC allows customers to keep their DIDs, calling plans, and rates with their current carrier. The customers' designated carrier provides all regulated telecommunications services and is responsible for telecommunications regulatory compliance.
    - **Additional features.** In addition to the functionalities described above, other features available within Zoom Phone include the following: unlimited extension-to-extension calling (on-net access), auto attendant/interactive voice response (IVR), call routing, call queuing, music on hold, call history, caller identification (outbound and inbound), call forwarding, call transfer, voicemail, and

call recording. Additional functionality such as enabling common area phones, and additional Toll Free and DID phone numbers may be purchased.

- **Nomadic Emergency ER Alert Service.** Nomadic emergency services provide the ability to dynamically detect and report phone users' location for emergency calling (for example, when you dial 9-1-1). To enable this feature, either you or the administrator must first define locations and, if required, sub-locations and a specific emergency address for each one (e.g. full address and floor number). Prior to your emergency address being provided to emergency services, you will be shown what information would be provided to emergency services providers.
- **Virtual Desktop Infrastructure (VDI) Thin Layer Plugin: IP Address.** VDI is a server-based computing model that allows the provision of a desktop image - over a network - to an endpoint device. Users can then access the operating system (OS) and applications on that endpoint. If you are running in a VDI environment, the IP address of the machine where the VDI Thin Layer Plugin is installed can be used to provide current location information to assist emergency services.
- **Third-Party Integrations.** Zoom Phone may be initiated within a supported third-party software instance (for example, Salesforce, Azure Active Directory), enabling you to initiate and record Zoom calls without leaving the third-party application.
- **Connect to Zoom Meeting Service.** Customers can add a Zoom Meeting Service license in connection to their Zoom Phone license.

This Privacy Data Sheet does not apply to Zoom for Government, Zoom Meetings, Zoom Events or Zoom Apps. For further detailed information about our Services, please visit the "Solutions" section of our website.

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 authorized by the Zoom Customer in a written document.

Zoom processes Personal Data obtained through 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 Acceptable Use Policy.

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

- improving and optimizing 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 modeling (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 processed by Zoom

The Services enable Customers and users to connect and share information with an easy-to-use, secure, and innovative communications platform.

An overview including all details of Personal Data Zoom processes on your behalf when delivering the Services to you is available in our Privacy Statement.

If you use the Services through a Customer account holder (such as your employer or school), that account holder controls the processing of your Personal Data. Your account holder can access the Personal Data described in this document and use it subject to their own privacy statement and policies. In particular, account owners and admins can access all call recordings of phone users or call queues.

If you have questions about how or why your Personal Data is collected, the legal basis for processing, or requests concerning your Personal Data, please refer to your account holder's privacy statement and policies. Questions and queries should be addressed to your account holder or IT administrator.

Zoom Phone Services may be connected to a corresponding license to Zoom Meeting Services which are governed by such Meeting's privacy notice. Accordingly, if you participate in a meeting

hosted by a user from another account, the host's account controls any recordings, transcripts, or files shared during the meeting.

Zoom Phone groups the Personal Data it processes into the following categories: Customer Content, Diagnostic Data, Account Data (end users), Account Holder Data, and Support Data, Location Data, and Integration Data.

Customer Content Data

This is data provided by the Customer through use of the Service including all data the Customer chooses to record or share during a call, including call communication content, cloud recordings, call participant information, stored SMS/MMS information, stored call history, and address book information.

Call Communication Content. This will include:

- Audio of a call, as well as of voicemail.

Customer Initiated cloud recordings. This will include the following recordings if such recording is permitted by the Customer's administrator controls and selected by a call participant (depending on the settings enabled):

- Call recording,
- Call recording text file,
- Voicemail, and
- Voicemail greetings.

Call Participant Information. This will include:

- Phone number and associated information (such as country code) for the caller and the callee(s),
- Name (if available) associated with a phone number,
- Source and destination phone numbers, including use of extensions, and
- Time elapsed since the call started.

Stored SMS/MMS Information. This is data at rest (i.e. in storage) and will include:

- Content of SMS/MMS messages,
- Files exchanged via MMS,
- Images exchanged via MMS,
- Videos exchanged via MMS,

- SMS/MMS channel title, and
- Name of recipient.

Stored Call History. This is data at rest (i.e. in storage) and will include:

- Phone number and associated information (such as country code) for the caller and the callee,
- Source and destination phone numbers, including use of extensions,
- Name (if available) associated with a phone number,
- Date of call,
- Time of call, and
- Duration of call.

Address book Information. This includes contact information made available through Customer controlled integrations (e.g. Outlook, Azure Active Directory) or importation (e.g. CSV file).

Diagnostic Data

Diagnostic Data includes all data automatically generated or collected by Zoom about the use of Zoom Phone. ***Diagnostic Data does not include a Zoom user's name, email address, or Customer Content Data.*** Diagnostic Data is made up of these categories of data, Call Metadata SMS/MMS Metadata, Voicemail Metadata, Voice Recording Metadata, Telemetry Data, and Other Service Generated Data.

Call Metadata

Call Metadata are metrics about Service usage, including when and how calls were conducted and quality of service. This category includes:

- Call ID
- System generated identifiers, including UUID of the caller and callee,
- Date and time of call,
- Duration of call,
- Source and destination phone numbers, including extensions,
- Type of call (inbound, outbound, toll-free),
- Call cost (based on per-minute rate),
- Version of the Zoom software running on an end user's device (client),

- Operating system and device information, including OS version, connection type (Wi-Fi, etc.), device make and device model),
- IP address (where applicable),
- ISP information (where applicable),
- Call result (busy, no answer, connected, missed, rejected, blocked, voicemail, error, redirected),
- Billing information, including account number, cost center, and department, if any,
- PSTN carrier information,
- Call queue information, if any, and
- Emergency services calling information.

SMS/MMS Metadata

- System generated identifiers, including conversation ID, message ID, and session ID,
- Name and email, if available in association with a phone number,
- Media file name, type, and size (when sending media),
- Source and destination phone numbers, including extensions,
- Message carrier identification,
- Message creation and expiration times,
- Read status, and
- Billing information, including account number, plan type, payment type, cost center, and department, if any

Voicemail Metadata

- System generated identifiers, including voicemail ID, account ID, and user ID,
- Message status and priority,
- Start and end times,
- Source and destination phone numbers, including extensions,
- Voicemail URL, and
- Transcript availability and storage.

Voice Recording Metadata

- System generated identifiers, including recording ID, account ID, and user ID,
- Recording status and priority,
- Start and end times,
- Recording type,
- Source and destination phone numbers, including extensions,
- Recording URL, and

- Transcript availability and storage.

Telemetry Data

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

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, and
- Call ID.

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 and push notifications.

Other Service Generated Data includes a Zoom persistent unique identifier that Zoom's Trust and Safety Team combines with other data elements including IP address, data center, PC name,

microphone, speaker, 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 with a need to know and subject to appropriate technical and organizational measures.

Account Data (end-user)

This is information associated with end-users who are members of a Zoom Phone account. Depending on how the account administrator has configured the Zoom Phone account, this information will include:

- Zoom unique user ID,
- Profile picture (optional),
- Display name, and
- Customer authentication data,
- Phone number and extension,
- Time Zone, and
- Language.

Account Holder Business Data

Account Holder Business Data is made up of two categories of data: Billing and Sales Data and Know Your Customer Data.

Billing and Sales Data

This is information associated with the individual(s) who are the billing and or sales contact for a Zoom Phone account. This will include:

- 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.

Zoom uses this information for very limited purposes including to:

- Create a Zoom account,
- Provide Zoom services,

- Respond to requests for support,
- Provide announcements related to software updates, upgrades, and system enhancements, and
- Send marketing communications, where permitted.

Know Your Customer Data

In order to provision Zoom Phone numbers, Zoom may need to collect additional information from the Account Holder based on your jurisdiction in order to satisfy local laws and regulations. This may include, when applicable:

- Government ID,
- Proof of business registration, and
- Proof of business address.

Support Data

Support data is information provided by a Customer to Zoom 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 Phone 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.

Location Data

Location Data is made up of two categories of data, Approximate Location, and Location Information.

Approximate Location

We collect your approximate location automatically through the use of our Services. This is information associated with the end-user's nearest city or town. This is used in order to:

- Comply with applicable privacy and other laws – for example, so we can provide you with the right notices for your area,
- Suggest choices such as language preferences,

- Monitor performance of our data centers and networks, and
- Route support requests.

Location Information

In order to assist nomadic emergency services (for example, 911) when you contact such emergency services, we collect your emergency address information. Such information is shared with your admin. In the event of an emergency call, it may be shared with the public safety answering point (such as 911) and members of the account's Internal Safety Response Team (if set up by your admin).

Nomadic emergency services enables Zoom to assist in determining your location, and is used only for purposes of responding to your emergency calls. If this feature is enabled by your admin, you may see an email or desktop client notification asking you to enable location sharing so that first responders can better respond to your emergency calls. After you enable location permission, you may also need to add or update your emergency address that is passed to first responders.

After adding or updating an emergency address for your location, Zoom Phone will automatically save the IP address or wireless access point identifiers for the location. Your IP address is collected so that when you place an emergency call from a defined location, the associated emergency address will be sent to emergency responders. If you are running in a VDI environment, your IP address is collected through the VDI Thin Layer Plugin.

Integration Data

If you have enabled integration of Zoom Phone with Salesforce (or other supported third party platform), you may launch Zoom Phone directly within your Salesforce instance, meaning you can initiate and record Zoom calls without leaving Salesforce. Such integration will enable a bi-directional data sync between Zoom and Salesforce (or other supported third party platform which you have enabled integration with Zoom Phone). For example, if you receive a call on Zoom Phone through Salesforce, a new lead/contact entry can automatically be generated in Salesforce; whereas if you reach out to an existing lead/contact, the associated record page will be retrieved for you to work on.

IV. Automated decision making

The personal data processed by the Services do not produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely on automated processing.

Zoom's systems do however have anti-fraud measures in place to block suspicious calls based on automated processing, as do our underlying service providers. In addition, our anti-fraud systems detect possible patterns that can suggest that there may be fraudulent conduct with regards to your account, in which case the system will warn you in order for you to verify recent activity.

V. 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 Zoom Phone 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 further information about these recipients in Section VIII. Subprocessors in this Privacy Data Sheet.

VI. Government Requests to access Personal Data

Zoom is committed to protecting our Customers and users' privacy and only produces user data to governments in response to valid and lawful requests, in accordance with 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.

VII. 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 centers and public cloud data centers, 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 center nearest the user sending or receiving the data.

Generally, Zoom lets Customers make choices about the data centers that process their 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. ***However, the selections do not apply to Zoom Phone or related features. The selections also do not impact the location of data at rest.*** For further information on selection data center regions, please see this Help Article.

Data at rest

Customer Content, Account Data, and Diagnostic 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.

VIII. Subprocessors

When Zoom hires a supplier to process Personal Data in order to provide some aspect of the Services to you, these suppliers are identified as a "Subprocessor" (in accordance with GDPR terminology), and are disclosed on Zoom's Subprocessor webpage.

Zoom's process for contracting with third-party subprocessors

Zoom requires its Subprocessors to process your Personal Data in accordance with the 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 data 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.

IX. 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 certifications and standards 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/IEC 27001:2013 Certification
- SOC 2 + HITRUST Attestation
- CSA STAR Level 2 Attestation
- UK Cyber Essentials Plus Certification

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