**DATA TRANSFER IMPACT ASSESSMENT**

On July 16, 2020, the Court of Justice of the European Union ("**CJEU**") issued its ruling in the case of the Irish Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) ("**Schrems II**").

The ruling invalidated reliance on the EU-US Privacy Shield Framework as a lawful means to transfer personal data from the European Economic Area ("**EEA**") to the United States, while also affirming the EU Standard Contractual Clauses as a valid data transfer solution.

This is a living document and Zoom will continue to update it. The document has been prepared for Zoom's enterprise customers in order to help our customers perform the data transfer impact assessment pursuant to the Schrems II decision.

This document 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.

| **A. OVERVIEW OF THE DATA TRANSFER PERFORMED** | |
|---|---|
| **Brief description of envisaged transfer** | Zoom Video Communications, Inc. ("**Zoom**") processes personal data in order to provide phone communication services to its customers. |
| **Current legal mechanism for the international transfer** | The European Standard Contractual Clauses (SCC), as issued by the European Commission on 4 June 2021. |
| **Describe the nature, scope and context of the data processing** | Basic processing activities for delivering Zoom's cloud-based phone service that uses voice over internet protocol ("VoIP") to provide two-way voice calling and private branch exchange functionality ("PBX").<br><br>It is offered through a unified app for phone, video, meetings and chat, and provides internal business VoIP and PBX functionality. In particular, the Zoom Phone software enables on-net calls and provides access to a range of Zoom call management features and functions.<br><br>Other processing activities include nomadic emergency services (calling emergency services and providing emergency address information to first responders so that they can provide assistance) as well as answering and initiating calls through the integration into Salesforce (and other supported third-party platforms). |

| | |
|---|---|
| **Categories of personal data processed** | The personal data processed by Zoom Phone can be classified into the following categories: Customer Content, Diagnostic Data, Account Data (end users), Account Holder Data, and Support Data, Location Data, and Integration Data.<br>● **Customer Content:** 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.<br>○ **Customer Initiated Cloud Recordings (optional):** this will include the following recordings if such recording is permitted by the Customer's administrator controls and initiated by a call participant (depending on the settings enabled): Call recording, Call recording text file, Voicemail, and Voicemail greetings<br>○ **Call Communication Content:** this will include the audio of a call, as well as of voicemail.<br>○ **Call Participant Information:** this will include the phone number and associated information (such as country code) for the caller and the callee(s), the name (if available) associated with a phone number, the source and destination phone numbers, including use of extensions, and the time elapsed since the call started.<br>○ **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 the name of the recipient.<br>○ **Stored Call History**: this is data at rest (i.e. in storage) and will include the phone number and associated information (such as country code) for the caller and the callee, the source and destination phone numbers, including use of extensions, the name (if available) associated with a phone number, the date of call, the time of call, and the duration of a call.<br>○ **Address book Information**: this includes contact information made available through |

| | |
|---|---|
| | Customer controlled integrations (e.g. Outlook) or importation (e.g. CSV file).<br>• **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 the following categories of data, Call Metadata SMS/MMS Metadata, Voicemail Metadata, Voice Recording Metadata, Telemetry Data, and Other Service Generated Data. Additional information on these categories of data can be found in the Zoom Phone Data Privacy Sheet.<br>○ **Call Metadata**: these 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.<br>○ **SMS/MMS Metadata**: these are 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).<br>○ **Voicemail Metadata**: this includes 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.<br>○ **Voice Recording Metadata**: this includes 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.<br>○ **Telemetry Data**: this 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.<br>○ **Other Service Generated Data:** this 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. It 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.<br>• **Account Data (end users):** 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.<br>● **Account Holder Business Data:** this is made up of two categories of data: Billing and Sales Data and Know Your Customer Data.<br>○ **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 the 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.<br>○ **Know Your Customer Data**: in order to provision Zoom Phone numbers, Zoom may need to collect additional information from the Account Holder based on jurisdiction in order to satisfy local laws and regulations. This may include, when applicable: a Government ID, Proof of business registration, and Proof of business address.<br>● **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.<br>● **Location data:** Location Data is made up of two categories of data, Approximate Location, and Location Information.<br>○ **Approximate Location:** Zoom collects |

| | |
|---|---|
| | approximate location automatically through the use of the 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 that Zoom can provide the right notices for the relevant area, Suggest choices such as language preferences, Monitor performance of data centers and networks, and Route support requests.<br>○ **Location Information:** In order to assist nomadic emergency services (for example, 911) when such emergency services are contacted, Zoom collects emergency address information. Such information is shared with the user's 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 the 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 the admin, an email or desktop client notification will appear asking the user to enable location sharing so that first responders can better respond to such emergency calls. After location permission is enabled, there may also be a need to add or update the emergency address that is passed to first responders. After adding or updating an emergency address for the location, Zoom Phone will automatically save the IP address or wireless access point identifiers for the location. The IP address is collected so that when an emergency call is placed from a defined location, the associated emergency address will be sent to emergency responders. If a VDI environment is enabled, the IP address is collected through the VDI Thin Layer Plugin.<br>● **Integration data:** Such integration will enable a bi-directional data sync between Zoom and the supported third party platform (e.g. Salesforce) in which integration with Zoom Phone has been enabled. For example, if a call is received on Zoom Phone through Salesforce and integration of Zoom Phone within Salesforce has been enabled, then upon receiving a call, a new lead/contact entry can |

| | |
|---|---|
| | automatically be generated in Salesforce. In addition, upon reaching out to an existing lead / contact, the associated record page on Salesforce will be retrieved. |
| **The recipients of the personal data** | • Zoom is the recipient of the data.<br>• Emergency services (if the user makes an emergency call to emergency services).<br>• Salesforce or other third-party platform (if the user enables such an integration).<br>• A list of entities engaged by Zoom to perform certain processing activities in order to facilitate the provision of our services can be found at the following address: https://zoom.us/subprocessors. |
| **What is the reason the processing of data is performed outside of the European Economic Area ("EEA")?** | In order to be able to provide a seamless 24/7/365 service to our customers around the world (so-called "follow-the-sun" operations), Zoom may need occasional, temporary access to customers' personal data from outside the EEA through a secure remote access environment for the following purposes:<br>• Enabling the phone call to be made;<br>• Enabling integration with third-party platforms pursuant to integration request from user;<br>• Providing 24/7/365 customer support; and<br>• Monitoring / maintenance of the software-as-a-service applications and the underlying infrastructure to securely operate the service. |

| B. REGULATORY FRAMEWORK | |
|---|---|
| **Is the data recipient (Zoom) located in the EEA? Are the entities engaged by Zoom to perform processing activities located in the EEA?** | No. Zoom is located outside the EEA (i.e. in the United States of America).<br>Entities engaged by Zoom to perform certain processing activities on behalf of Zoom (https://zoom.us/subprocessors) are also located outside the EEA (i.e. in the United States). |
| **Is Zoom aware of any applicable laws in the recipient country that could constitute an obstacle to its ability to comply with appropriate safeguards pursuant to European data protection laws?** | Yes. The United States has implemented law enforcement and state security-related legislation that could be used to compel a US-based cloud provider, such as Zoom, to disclose customers' personal data to law enforcement or state security agencies in a way that is contrary to its customers' processing instructions.<br><br>These powers to compel disclosure could arise under section 702 of the Foreign Intelligence Surveillance Act (FISA) as further described below.<br><br>In addition, the US Government has adopted Executive Order 12333 (EO 12333), which permits the US national security agencies to conduct surveillance outside of the US, which may include exploiting vulnerabilities in telecommunications infrastructure to access data in transit to the US, as further explained below. |

| | | |
|---|---|---|
| **Risks posed by laws that authorize government authorities to access or conduct surveillance for security or other reasons** | ***Foreign Intelligence Surveillance Act ("FISA"), Section 702*** | Pursuant to section 702 of FISA, the government of the United States may compel "electronic communications service providers" to disclose information about non-US persons located outside the US for the purposes of foreign intelligence information gathering.<br><br>This information gathering is jointly authorized by the US Attorney General and the Director of National Intelligence, and must also be approved by the Foreign Intelligence Surveillance Court in Washington, DC.<br><br>Once approved, the US government sends relevant providers certain "selectors" (such as telephone numbers or email addresses) associated with specific "targets" (such as a non-US person or legal entity). In-scope providers must comply with these directives in secret and may not notify their users that they have received such directives. |

| | | |
|---|---|---|
| | ***Executive Order 12333 ("EO 12333") and Presidential Policy Directive 28 ("PPD- 28")*** | Pursuant to Executive Order 12333, US intelligence agencies (such as the US National Security Agency) may conduct surveillance outside of the US. In particular, it provides authority for US intelligence agencies to collect foreign "signals intelligence" information, which is information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means. This may for example include accessing underwater cables carrying Internet data in transit to the United States.<br><br>Executive Order 12333 does not rely on the compelled assistance of service providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure.<br><br>In addition, PPD-28 limits the use of signals intelligence collected in bulk to detecting and countering six types of threats:<br>a) espionage and other threats from foreign powers;<br>b) terrorism;<br>c) threats from weapons of mass destruction;<br>d) cybersecurity threats;<br>e) threats to U.S. or allied forces; and<br>f) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section. |

| | |
|---|---|
| **Is Zoom potentially within the scope of such security and surveillance powers? Please explain.** | Yes. Like any U.S. based cloud computing provider, Zoom is likely to qualify as a "remote computing service", and therefore be an "electronic communications service provider" within the scope of section 702 of FISA.<br><br>Pursuant to Executive Order 12333, there is a possibility that data transmitted to or from Zoom via means of telecommunications infrastructure outside the U.S. may be accessed by the U.S. government. However, Executive Order 12333 does not authorize the U.S. government to compel data importers to provide customer information or assist the government. Zoom does not voluntarily provide, and has not provided, information or assistance to the U.S. government in connection with its efforts to conduct surveillance under Executive Order 12333. |

| **C. ASSESSMENT OF THE DATA RECIPIENT'S APPROPRIATE SAFEGUARDS** | |
|---|---|
| **Has Zoom ever been subject to a law enforcement or other government agency request for access to EEA data? If so, how often?** | Yes, Zoom receives law enforcement requests from around the globe. We screen each international request carefully to ensure that we only respond to ones that are legally valid and appropriately scoped.<br><br>For more details, Zoom's transparency report is available at:<br>https://zoom.us/docs/en-us/transparency.html |

| | |
|---|---|
| **Could Zoom be subject to a request for access to data located in the EEA pursuant to FISA?** | The U.S. government – like other governments – may potentially request that Zoom provide data under applicable law. Nevertheless, it is important to highlight that the U.S. government's use of national security-related legal processes are limited to certain counterterrorism or foreign intelligence investigations.<br><br>While consumer-facing cloud and electronic communication services are prone to receiving national security requests due to the nature of the data they are processing within their systems (e.g. email or mobile communication content, social media content), enterprise cloud service providers like Zoom are less likely targets for national security requests. In particular, PPD-28 limits the collection of signal intelligence to certain core areas as described above. Given the types of information processed by Zoom, as well as Zoom's role as an enterprise cloud service provider, the number of any such requests in the future is likely to be very small. |
| **Is Zoom subject to Executive Order 12333?** | Executive Order 12333 does not authorize the U.S. government to compel data importers to provide customer information or assist the government. Zoom does not voluntarily provide information or assistance to the U.S. government in connection with its efforts to conduct surveillance under Executive Order 12333. |
| **Does Zoom have a documented government data access policy?** | Yes. Zoom has a robust policy in place that sets out how Zoom would respond to a request received from a law enforcement or government authority. Each request (if and when received) would be carefully reviewed by Zoom's Legal department on a case-by-case basis to determine if it is lawful, valid and enforceable and follows Zoom's policies. If Zoom believes that a request is overly broad, Zoom would seek to narrow it.<br><br>For more details on our government data access policy, our Government Requests Guide is accessible at: https://zoom.us/docs/en-us/government-requests-guide.html. |

| | |
|---|---|
| **Does Zoom refuse government access to data unless under a mandatory compulsion or where the data exporter has consented?** | Zoom does not disclose data to a law enforcement or other government agency unless where and to the extent compelled by law. Pursuant to Zoom's internal policy, Zoom does not disclose data on a voluntary basis. |
| **Will Zoom notify the affected customer about any request for government access to data, unless legally prohibited?** | Yes, pursuant to Zoom's internal policy, Zoom notifies any affected customer about any request for access to its data, unless explicitly prohibited by law.<br>For more information, see our Government Requests Guide available at https://zoom.us/docs/en-us/government-requests-guide.html. |
| **Does Zoom publish data access transparency reports?** | Yes. Zoom publishes semi-annual transparency reports that set out the number of government requests or demands it has received for user data.<br><br>Our first report is available at https://zoom.us/docs/en-us/transparency.html.<br><br>Our most recent report is available at https://explore.zoom.us/docs/en-us/trust/transparency.html. |
| | |

| **D. SECURITY MEASURES** | |
|---|---|
| **What security measures does Zoom have in place to mitigate the risk associated with data transfers?** | • We use Secure Real-time Transport Protocol leveraging Advanced Encryption Standard (AES)-256 GCM to encrypt and protect phone conversations in transit to and from our data centers.<br>• Connections between the Zoom client and Zoom's cloud use HTTPS and leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority.<br><br>For more details, please refer to the Zoom Encryption White Paper which is available here: https://zoom.us/docs/doc/Zoom%20Encryption%20Whitepaper.pdf. |

| | |
|---|---|
| **What other security measures are in place?** | • **Cloud Recording Storage**: Cloud Recordings are processed and stored in Zoom's cloud. These recordings can be available only to people in your organization.<br>• **Authentication**: Zoom offers a range of authentication methods such as SAML, Google Sign-in and Facebook Login, and/or Password based which can be individually enabled/disabled for an account.<br>• **2-Factor Authentication** ("**2FA**"): Admins can enable 2FA for your users, requiring them to set up and use 2FA to access the Zoom web portal.<br>• User Passwords are salted and hashed. |