FAQs:

International Data Transfers

Updated September 2021

How can EU companies transfer data to Zoom in the US?

Previously available mechanisms

Prior to the Summer of 2020, companies in the European Economic Area and UK had two main ways to transfer personal data to their US-based service providers (like Zoom):

1. *The Privacy Shield Framework*. The US service provider could certify under a privacy framework designed by the U.S. Department of Commerce, the European Commission and the Swiss Administration to provide companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States. This mechanism binds the data importing service provider to specific personal data protections and complaint mechanisms.
2. *The SCCs*. The EEA/UK data exporting company and the US data importing service provider could agree to the European Commission's so-called "Standard Contractual Clauses" (referred to herein as the "old" SCCs), which were designed to protect personal data leaving the European Economic Area (EEA) through contractual obligations and protect data subject rights. In effect, by entering into the old SCCs, both parties contractually agreed to protect the data in accordance with EU data protection standards.

However, on July 16th, 2020, the Court of Justice of the European Union ("CJEU") invalidated the EU-U.S. Privacy Shield in its ruling in the case of the *Irish Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case c-311/18), also known as the "Schrems II ruling". The ruling also affirmed the old SCCs as a valid data transfer solution as long as certain conditions are met.

Then, on September 8th 2020, the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland issued an opinion concluding that the Swiss-U.S. Privacy Shield Framework does not provide an adequate level of protection for data transfers from Switzerland to the United States pursuant to Switzerland's Federal Act on Data Protection (FADP).

Current primary data transfer mechanism

Following the Schrems II ruling, EEA and UK data exporting companies were left with entering into the old SCCs as the primary mechanism for transferring data to the US.

On June 4th 2021, the European Commission formally adopted the *new* SCCs which incorporate the requirements laid out in the European General Data Protection Regulation (GDPR) and the Schrems II ruling (the "new" SCCs).

The European Commission granted companies a grace period of 18 months to implement the new SCCs in connection with their existing contracts. New contracts are required to incorporate the new SCCs from September 27th, 2021.

Zoom has welcomed the adoption of the new SCCs, which ensure consistency with the GDPR and the Schrems II ruling and is working to update its contracts to incorporate these new standards within the applicable grace periods.

Does Zoom offer the EU Standard Contractual Clauses (SCCs)?

Yes. Zoom will sign SCCs with any EEA or UK enterprise customer that uses its services. At present, Zoom is continuing to rely on the old SCCs for transfers of EEA/UK customer data under existing customer contracts. In the coming months, we will update such agreements to implement the new SCCs, within the grace period permitted by the European Commission.

Any new enterprise customer contracts will incorporate the new SCCs from September 27th, 2021.

How can I get a copy of Zoom's Standard Contractual Clauses

Enterprise customers can access Zoom's pre-signed "old" SCCs here. Generally speaking, the old SCCs were automatically incorporated into your online terms of service with us or by way of a separate mutually executed Data Processing Addendum ("DPA"), where you have executed a separate Master Subscription Agreement with Zoom.

The "new" SCCs are incorporated into Zoom's recently updated DPA (here) by reference. The full text of the new SCCs can be accessed on the European Commission's website here.

Going forward, new enterprise customers will be invited to sign-up to the updated DPA terms. In due course, we will also make available an amendment agreement that existing enterprise customers can download and countersign to update their current DPA with us, giving all customers the opportunity to enter into the new SCCs with Zoom.

Enterprise customers can request a copy of the SCCs or our DPA by emailing privacy@zoom.us.

What was the Schrems II ruling about?

The Schrems II ruling arose out of a complaint made by an Austrian data subject, Maximillian Schrems, to the Irish Data Protection Commissioner, concerning transfers of his personal data to the United States and the potential for his data to be accessed by US government agencies. The case was referred by the Irish Data Protection Commissioner to the Irish High Court, which in turn referred certain questions up to the CJEU for clarification.

In its ruling, the CJEU ruled that the EU-US Privacy Shield, a self-certification program relied upon by more than 5,000 US data importing organisations, no longer provided a lawful means to transfer personal data from the EEA and UK to the United States. As a result, organisations that previously relied upon the EU-US Privacy Shield to transfer EEA and UK personal data to the US now need to move to another lawful solution.

The CJEU also ruled that the European Commission's "Standard Contractual Clauses" (i.e. the "old SCCs") did remain a lawful mechanism for transferring personal data from the EEA and UK to non-EEA countries. However, the CJEU further ruled that, before transferring personal data from the EEA/UK to a non-EEA country, the data exporter and data importer must assess whether the personal data to be transferred will be protected to a standard which is "essentially equivalent" with EU data protection rules, taking into account the protections afforded by the SCCs and the relevant aspects of the legal system of the recipient country.

What is required in the wake of the Schrems II ruling?

As explained above, the Schrems II ruling requires that data exporters and importers each undertake an assessment of their contemplated transfer(s) (also known as a "data transfer impact assessment") in order to establish whether, in the importer's jurisdiction, an "essentially equivalent" level of protection can be afforded to the data transferred. This involves an assessment of the types of data transferred, applicable laws of the data importer jurisdiction and the measures in place to protect the data (including, the "transfer tool" utilized by the parties to make the transfer in compliance with the GDPR; e.g., the SCCs).

While the "old" SCCs were confirmed by the Schrems II ruling as being a valid mechanism for data transfers, the European Commission had already indicated its intention to update the old SCCs to bring them in line with the GDPR's requirements. Accordingly, the "new SCCs" (here) were published in June 2021 (effective starting from June 27, 2021) and provide for more robust protections as required by the GDPR.

In addition to the European Commission's publication of the new SCCs, on June 18, 2021 the European Data Protection Board published its recommendations (here) on assessing the need for so called "supplemental measures" (i.e., additional measures to protect data where the outcome of a data transfer impact assessment indicates that an essentially equivalent level of protection is not available). The recommendations set out the steps the parties should consider when conducting a data transfer impact assessment.

Does Zoom help customers conduct data transfer impact assessments?

Yes. Zoom has prepared a data transfer impact assessment information sheet (here). This document has been prepared to help Zoom's customers perform their own data transfer impact assessments, pursuant to the Schrems II ruling.

What "safeguards" does Zoom provide (in addition to the use of the Standard Contractual Clauses)?

The security measures we use to ensure the security of communications sent over and stored on Zoom's platform include the following:

- Encryption: The connection between your device and Zoom is encrypted, using a mixture of TLS (Transport Layer Security), Advanced Encryption Standard (AES) 256 bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used will depend on whether you are using the Zoom client, a web browser, a third party device or service, or the Zoom phone product. For further information, please see our Encryption Whitepaper.
- Controlled data routing: Controlled data routing that allows for opting in or out of a specific data center region for data in transit. Enterprise account owners and admins on paid accounts can customize which of our data center regions (excluding their home region) to use for hosting their real-time meeting and webinar traffic.
- Transparency: Transparency on data routing via the account administration dashboard.

- Protections against unauthorised meeting participants: Safeguards and controls to prohibit unauthorized participants such as:
    - Eleven (11) digit unique meeting IDs;
    - Complex passwords;
    - Waiting Rooms with the ability to automatically admit participants from your domain or another selected domain;
    - Meeting lock feature that can prevent anyone from joining the meeting;
    - Ability to remove participants; and
    - Authentication profiles that only allow entry to registered users, or restrict to specific email domains.
- Selective meeting invitation: The host can selectively invite participants via email, IM, or SMS. This provides greater control over the distribution of the meeting access information. The host can also create the meeting to only allow members from a certain email domain to join.
- Meeting details security: Zoom retains event details pertaining to a session for billing and reporting purposes. The event details are stored at the Zoom secured database and are available to the customer account administrator for review on the customer portal page once they have securely logged-on.
- In-meeting security: During the meeting, Zoom delivers real-time, rich-media content securely to each participant within a Zoom meeting. All content shared with the participants in a meeting is only a representation of the original data. This content is encoded and optimized for sharing using a secured implementation as follows:
    - Is the only means possible to join a Zoom meeting;
    - Is entirely dependent upon connections established on a session-by-session basis;
    - Performs a proprietary process that encodes all shared data;
    - Encrypts all real-time media (audio, video, screen sharing) using the AES encryption standard;
    - Encrypts other data using TLS encryption standard; and
    - Provides a visual identification of every participant in the meeting.
- Host controls: Meeting host controls can enable/disable participants from content sharing, chat and renaming themselves.
- Reporting: Report a user feature enables the meeting host to flag problematic behavior.
- In-product security controls: Security controls with a dedicated Security icon on the main interface.
- Role-based user security: The following pre-meeting security capabilities are available to the meeting host:
    - Secure log-in using standard username and password or SAML single sign-on;

- Start a secured meeting with passcode; and
- Schedule a secured meeting with a passcode.

- Application security: Zoom can encrypt all real-time media content at the application layer using Advanced Encryption Standard (AES).
- Zoom client group policy controls: Specifically applicable to the Zoom Meetings client for Windows and Zoom Rooms for Windows, administrators can define a broad set of client configuration settings that are enforced through active directory group policy controls.
- Administrative controls: The following security capabilities are available to the account administrator:
  - Secure login options using standard username and password (with the option to enable two-factor authentication as an added layer of security), or SAML SSO;
  - Add user and admin to account;
  - Upgrade or downgrade account subscription level;
  - Delete user from account;
  - Review billing and reports; and
  - Manage account dashboard and cloud recordings
- Encryption: End-to-end encryption may be enabled to ensure that communication between all meeting participants in a given meeting is encrypted using cryptographic keys known only to the devices of those participants. This ensures that no third party — including Zoom — has access to the meeting's private keys. All cloud recordings are encrypted using AES 256 bit encryption with complex passwords on by default.
- Robocall prevention: Prevent robocalling with rate limiting and reCAPTCHA (requires human intervention) enabled across all platforms.
- Fingerprinting: Audio recordings with a user's electronic fingerprint embedded into the audio as an inaudible watermark.

Does Zoom give customers' data to the US Government?

Zoom has a robust process for responding to any government request for customer data, regardless of the country. A government request occurs when a government agency, such as law enforcement, a state security body, or another public authority, contacts Zoom to obtain certain data about Zoom users.

There are two general types of government requests: (1) voluntary, meaning that the government agency asks Zoom to disclose customer data, but does not legally require us to do so, and (2) mandatory, meaning that the government agency has the legal authority, usually through a court order to require Zoom to disclose customer data.

Zoom does not disclose customer data in response to voluntary government requests, except in emergency situations as explained below. Otherwise Zoom only discloses customer data in response to a mandatory request and after Zoom's law enforcement team reviewed the

government demand to ensure the requests' validity, and then only provides that data specified in the legal order.

For example, when Zoom receives a government request, we first check that it has been properly issued pursuant to applicable laws and rules and through appropriate official channels, including by requiring an official, signed document, or, where a request is made by email from a government agency, by checking it has been transmitted from the official email address of that government agency.

We provide more detail on how Zoom will respond to requests for personal data from government agencies (in the US and elsewhere) in our Government Requests Guide that is available here or our Government Requests FAQs that is available here.

Does Zoom enable anyone to "eavesdrop" on my Zoom call or meetings?

No. Zoom does not have a mechanism to decrypt live meetings for any purpose, and we do not have the means to insert our employees or others into meetings without that person being visible as a participant. As such, we do not collect or maintain information on meeting content unless requested by the meeting host, for example, to record and store the meeting in our cloud.

How does Zoom respond to government requests for data?

Zoom's legal team reviews all government requests for data and will only disclose such data if legally compelled to do so (other than in emergency situations) and then, only in accordance with the applicable legal process. If a request is vague or overly broad, Zoom will challenge it.

We provide more detail on how Zoom will respond to requests for personal data from government agencies (in the US and elsewhere) in our Government Requests Guide that is available here or our Government Requests FAQs that is available here.

Will Zoom notify me if it gets a request for my data?

Yes, unless legally prohibited. Our policy is to notify users of requests for their information and provide a copy of the request unless we are legally prohibited from doing so. For more information, see our Government Requests Guide that is available here or our Government Requests FAQs that is available here.

Is Zoom subject to s.702 FISA or to EO12333?

The Schrems II case focussed on concerns that US government agencies can, in certain circumstances, compel US-based service providers to disclose EEA personal data in a way that is not "essentially equivalent" with EEA data protection rules. The judgment cited two main US legal regimes in this respect: Section 702 of the Foreign Intelligence Surveillance Act (as amended) ("FISA"), and Executive Order 12333 ("EO1233").

FISA regulates surveillance of non-US persons located outside of the US. Under FISA, "electronic communications service providers" can be compelled by the Foreign Intelligence Surveillance Court to disclose certain data. Most, if not all, US-based providers of cloud-based technology solutions will fall within the scope of an "electronic communications service provider". Zoom is no different in this respect.

EO12333 is an executive order that authorises intelligence agencies to conduct surveillance outside of the US, and it does not rely upon compelled assistance from service providers. As such, Zoom is not directly subject to EO12333.

There are controls around how US government agencies can obtain signals intelligence. In 2014, President Obama issued Presidential Policy Directive 28 (“PPD-28”) which directed US intelligence agencies to review their policies regarding the treatment of non-US persons in connection with signals intelligence programs. Effectively, PPD-28 imposes restrictions on signals intelligence activities, including those conducted under section 702 of FISA and EO 12333, regardless of the target's nationality or location.

Nevertheless, Zoom has decided to take the supplementary measures outlined above. These supplementary measures should mend any potential deficiency in the level of data protection provided to the personal data that is transferred.

Why not just stop sending data to the US?

Think about it: if we did that, how would Zoom users be able to communicate with their colleagues, friends and family members in the US? Worldwide data transfers are essential for any global communications service provider that enables cross-border communications – whether by traditional telephone, Voice over IP, email and SMS, or video conferencing.

In addition, Zoom is a US headquartered company, and the majority of our operations therefore take place in the US. Rest assured though: we take the privacy, security and confidentiality of our users very seriously and, wherever your data is processed, we will protect it in accordance with our privacy statement and as described in these FAQs.

Will Zoom publish transparency reports?

Yes. Zoom publishes transparency reports that set out the number of government requests or demands it has received for user data. In December 2020, we issued our first transparency report which covers government requests that we processed between May 1, 2020 and December 12, 2020. We intend to continue publishing new reports semi-annually beginning in 2021. For more information, see our Transparency Report page available here.

If you have any further questions about how Zoom protects your personal data, please contact privacy@zoom.us