Updated May 2022

Slack transfer impact assessment white paper

slack

Table of contents

Introduction: How to use this document

Trust is our number one value, and nothing is more important than the privacy and security of our Customers' data. We will always protect our Customers' data, while complying with applicable laws. We see Customer compliance as a shared responsibility between Slack and its Customers. This document summarizes how **Customers can use the Slack Service to transfer their data in compliance with European law** by relying on the industry-leading contractual, technical and organizational frameworks and safeguards we have in place (Slack Service is defined in the **Slack Trust and Compliance Documentation**). It is intended to assist Customers in performing their own transfer impact assessments with regard to their use of the Slack Services. This document explains the measures taken by Slack to ensure that an equivalent level of protection exists for Personal Data that is transferred out of the European Economic Area (EEA), Switzerland and the U.K. (together, "Europe") in connection with use of Slack Services. This document also provides an overview of the assurances made by Slack to protect its Customers' data from inappropriate disclosure to law enforcement and intelligence agencies.

Unless otherwise defined, capitalized terms in this document are defined as set forth in the Slack **Data Processing Addenda** (DPA).

For the avoidance of doubt, this document should not be used to assess customer-specific use cases, as the impact of processing Personal Data depends on the context of data usage by the Customer and the Customer's particular deployment of the Slack Services. Only our Customers are in a position to know and independently assess such specific use cases. Customers are responsible for ensuring that their use of the Slack Services complies with their legal and contractual obligations.

Background: The Schrems II ruling and EDPB recommendations

At Slack, we believe that conducting a Data Protection Impact Assessment (DPIA) is a helpful part of an overall privacy program to identify privacy risks, document compliance with applicable laws and internal policies, and maintain customer trust.

Schrems II ruling

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued its ruling in the "Schrems II" case.[1] In that ruling, the CJEU invalidated the EU-U.S. Privacy Shield framework as a mechanism for lawful transfers of personal data from the EU to the U.S. At the same time, the CJEU confirmed that the European Commission's standard contractual clauses (SCCs) continue to be a valid legal mechanism for the transfer of personal data from Europe to non-adequate countries ("Third Countries"), while stipulating stricter requirements for those transfers. It held that companies are responsible for conducting diligence to help ensure compliance with European data protection laws, including assessing whether there is a level of protection for the personal data transferred that is essentially equivalent to that guaranteed by the GDPR, the EU Charter of Fundamental Rights and the broader EU legal order. Companies transferring personal data out of Europe to Third Countries (data exporters) must carry out these assessments. In the Schrems II ruling, the CJEU also confirmed that, depending on the outcome of the above assessment, companies may need to put in place supplementary measures to ensure that there is an essentially equivalent level of protection for personal data transferred to Third Countries.

EDPB recommendations

After the Schrems II decision, the European Data Protection Board issued non-legally-binding recommendations (the "EDPB recommendations")[2] that created a non-exhaustive list of protections companies can take when transferring personal data from Europe to Third Countries to ensure an essentially equivalent level of protection for the data that is transferred. The EDPB Recommendations endorse the following six-step data transfer assessment (EDPB Transfer Impact Assessment):

Step 1: Identify international data transfers. Perform a mapping of international data transfers and assess whether the data transferred is adequate and limited to what is strictly necessary for the purpose for which it is transferred.

[1] Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Step 2: Identify data transfer mechanism(s). Verify the transfer tool(s) on which the transfer relies.

Step 3: Assess the laws or practices of the third countries. Assess whether local laws or practices may impinge on the effectiveness of the appropriate safeguards of the transfer tool(s), including using Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Step 4: Adopt supplementary measures. If the laws or practices of the Third Countries mean that the use of the transfer tool(s) alone would not provide an essentially equivalent level of protection, identify the supplemental contractual, technical or organizational measures that are necessary to bring the level of protection of the data transferred up to the European standard of essential equivalence.

Step 5: Adopt necessary procedural steps. Take any formal procedural steps that the adoption of any supplementary measure(s) may require.

Step 6: Re-evaluate, at appropriate intervals, the level of protection afforded to the data that the data exporter transfers to Third Countries, and monitor if there have been or there will be any developments that may affect it.

Description of transfers

This section helps Customers perform step 1 of the EDPB Transfer Impact Assessment:

Step 1: Identify international data transfers.

Below, we describe the scenarios where personal data may be transferred from Europe to Third Countries in connection with the use of Slack Services.

A. Customer support

Purpose and details of the transfer

Slack provides 24/7 customer support using a "follow the sun" model. Slack is a geographically distributed entity and has offices and employees located throughout the world who support the delivery of our services. Further information on **Slack affiliates** can be found on the Slack affiliates page.

Unless specifically authorized by the Customer, Slack support staff do not have access to the Customer's Slack environment. The Customer's users may choose to provide the Slack support team with information on their Slack instance.

The frequency of any transfers of Personal Data for customer support purposes depends on the number and type of support queries raised by the Customer. The locations from which customer support may be provided are set out in the **Salesforce Infrastructure and Sub-processors documentation** (see section on Slack) and **Slack affiliates** page.

Categories of personal data transferred

The categories of Personal Data that may be transferred for this purpose depend on the nature of the support case, the level of access provided by the Customer, and the categories of Personal Data submitted to the Slack Services by the Customer. They may include:

- User email address
- User name
- User account information
- Billing details
- All other data submitted by Customers to a support ticket

B. Technical operations

Support purpose and details of the transfer

To respond to technical or service problems, a dedicated team of Slack database administrators may, on occasion, require remote access to the database tables on which Customers' Personal Data is hosted, following strict access and monitoring controls.

The following operations may involve accessing the raw data (also see section 5 below) contained in the database:

- Management of servers, connections and networks
- Providing technical and networking service
- Maintaining operations
- Troubleshooting hardware issues
- Quality assurance testing

Locations from which technical operations support is provided

The locations from which technical operations support may be provided are set out in the **Salesforce Infrastructure and Sub-processors documentation** (see section on Slack) and **Slack subprocessors page**.

C. Storage of personal data outside Europe

Purpose and details of the transfer

Slack is hosted on Amazon Web Services, and the default storage location is in the U.S. However, Slack offers Customers the ability to store certain types of Customer Data at rest in Europe and other regions. The data center hosting location applicable to each Slack Customer can vary depending on whether an organization uses Slack's **data residency feature** (available on Business+ plans or above). In line with Slack's data residency offering, Customers may select a data region, but certain Customer Data may be stored outside this region. To operate our Services, please also note that "Other Information," as defined in Slack's **Privacy Policy**, is stored in the U.S.

Locations outside of Europe where personal data may be stored

The current list of Sub-processors engaged in processing Personal Data for the performance of the Services, including a description of their processing activities and locations, is accessible **here**.

Categories of personal data transferred

The categories of Personal Data that may be transferred depend on the categories of Personal Data submitted to the Slack Services by the Customer and whether an organization uses Slack's **data residency feature**.

D. User information replication

Purpose and details of the transfer

When Users log in to the Customer's Slack environment, login requests will be sent to the U.S. The authentication process redirects the User to the U.S. data center for the duration of the active session. For Customers enrolled in Slack's **data residency** feature, Slack may temporarily store identifying information about Users across its data storage locations outside of Europe for the purpose of facilitating the login process.

Locations where user information may be temporarily stored

The locations where User information may be stored are set out in the **Salesforce Infrastructure and Subprocessors documentation** (see section on Slack) and **Slack subprocessors page**.

E. Content delivery networks

Purpose and details of the transfer

Content delivery networks ("CDNs") are utilized to optimize content delivery, as listed in the **Salesforce Infrastructure and Sub-processors documentation** (see section on Slack) and **Slack subprocessors page**. CDNs are commonly used systems of distributed services that expedite the transmission of content. Typically, a CDN is used to securely cache copies of content globally to better support end users of the Slack Services. Slack uses Amazon CloudFront as our primary CDN.

More information on CDN services can be found in the **Salesforce Infrastructure and Subprocessors documentation** (see section on Slack) and **Slack subprocessors page**.

Locations where customer data may be cached

More information on the locations where Customer Data may be cached (temporarily stored) can be found in the **Salesforce Infrastructure and Sub-processors documentation** (see section on Slack) and **Slack subprocessors page**.

Categories of personal data transferred

The categories of Personal Data that may be transferred depend on the categories of Personal Data submitted to the CDN by the Customer.

Transfer tools

This section helps Customers perform step 2 of the EDPB Transfer Impact Assessment:

Step 2: Identify data transfer mechanisms.

Slack provides support to our Customers for compliance with international data transfers by executing Standard Contractual Clauses ("SCCs") through our Data Processing Addenda ("DPA").

- Standard contractual clauses for the transfer of personal data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "2021 SCCs") are legal contracts entered into between contracting parties who are transferring Personal Data outside of the EU to Third Countries.

For further information, please see Slack's DPA, available **here**. The categories of Personal Data that may be transferred depend on the categories of Personal Data submitted to the Slack Services by the Customer and whether an organization uses Slack's **data residency feature**.

Potential privacy risks under local laws and relevant practice

This section helps Customers perform step 3 of the EDPB Transfer Impact Assessment:

Step 3: Assess the laws or practices of the third countries.

This section describes possible privacy risks with regard to potential inappropriate disclosure to law enforcement and intelligence agencies associated with the data transfers described above. This section also briefly elaborates on Slack's practical experience in this regard, which is relevant for Customers when assessing the actual risks.

Transfers to the United States

The Schrems II ruling has focused European attention on the breadth of law enforcement powers, particularly with respect to national security programs, that permit U.S. government agencies to engage in proactive surveillance. Slack recognizes that this has generated uncertainty about the impact of such U.S. laws on EU data transfers. To address these issues, we have set out specific information about certain U.S. laws considered by the CJEU ruling and their application to the Slack Services in this section.

Executive order 12333 ("EO 12333")

EO 12333 authorizes and governs surveillance activities by U.S. intelligence agencies. As the CJEU noted, the primary concern regarding EO 12333 is the U.S. government's ability to collect personal data while it is in transit to the U.S. by intercepting data traveling over transatlantic cables. Personal Data can effectively be protected from this type of interception through security measures such as encryption. Slack addresses this risk today by encrypting Personal Data and only transferring data that is subject to these strong protections. Please see section 5 below for more information about these measures. It is important to note that EO 12333 does not grant the U.S. government the ability to compel companies to provide assistance with the above activities. Moreover, Slack contractually commits to its Customers that it will not do so voluntarily. As a result, Slack does not and cannot be ordered to take any action to facilitate the type of bulk surveillance sought under EO 12333.

FISA section 702

Section 702 of the Foreign Intelligence Surveillance Act ("FISA Section 702") sets forth processes and conditions for U.S. intelligence agencies to lawfully collect information relating to non-U.S. persons who are reasonably believed to be located outside the U.S. if a significant purpose of such collection is to acquire foreign intelligence information and the source of the information is a U.S.-based electronic communication service provider ("ECSPs").

FISA Section 702 authorizes "upstream" and "downstream" collection.

Upstream collection authorizes U.S. authorities to collect communications as they travel over the internet backbone. Slack does not provide such backbone services, but only carries traffic involving our own Customers. As a result, Slack is not eligible to receive the type of orders principally addressed in, and deemed problematic by, the Schrems II ruling.

Downstream collection authorizes U.S. authorities to collect targeted data directly from ECSPs based in the U.S. To the extent that Slack may be compelled to respond to such a targeted request for Customer Data, we will carefully review the request to verify it is lawful and challenge the request in accordance with Slack's principles and contractual commitments on government access requests, as further described in section 5 below. More information on the surveillance program operated pursuant to FISA Section 702 can be found **here**.

U.S. clarifying lawful overseas use of data act ("CLOUD Act")

The CLOUD Act, enacted in 2018, clarifies existing legal frameworks and retains meaningful limitations on U.S. law enforcement's ability to request data, for example: Companies must be subject to the jurisdiction of U.S. law enforcement agencies. The CLOUD Act further confirms that the physical location of data is not the deciding factor but whether the recipient of a request has "possession, custody, or control" of the data. Requests are subject to the existing high standards and procedures for making such a request. Lastly, the CLOUD Act also established additional safeguards, including explicitly allowing companies to challenge disclosure requests that conflict with another country's laws. To the extent that Slack may be compelled to respond to such a law enforcement request for Customer Data, we will carefully review the request to verify that it is lawful and appropriate, including with respect to the data sought and relevant jurisdiction, and, when necessary, challenge the request in accordance with Slack's principles and contractual commitments on government access requests, as further described in section 5 below.

Relevant practice

The EDPB Recommendations also enable Customers to take into account Slack's practical experience "with relevant prior instances of requests for access received from public authorities" when performing their transfer impact assessment.

Slack's Transparency Reports show that Slack receives an overall low volume of compelled

disclosure demands from law enforcement entities, and very few requests from non-U.S. entities. In all circumstances, Slack requires proper domestication based on the law enforcement entity and the data sought. Please review our annual **Transparency Report** to learn more.

Where at all possible, in the interest of efficiency and expediency, Slack seeks to have data demands managed directly through the Customer and encourages requesting entities to work directly with the Customer. The Customer is best equipped to comply with a demand, given that they architect the unique configuration of their Slack instance and can control the subject matter, nature, purpose, type, and/or data subject categories related to a workspace. Further and to this end, Slack will notify Customers of compelled requests for data unless prohibited by law.

For more information regarding Slack's commitment to transparency and how we deal with government access requests, please see section 5 below.

In addition, we would like to point our Customers to the **white paper** from the U.S. Department of Commerce, Department of Justice, and Office of the Director of National Intelligence. The white paper outlines the limits and safeguards in the U.S. relating to government access to data in response to the Schrems II ruling.

In summary, Slack's relevant practice as demonstrated by the Transparency Report shows that the compelled disclosure scenarios that were flagged in the Schrems II ruling as potentially being high-risk with respect to the consumer service at issue in that case are in fact low-risk when it comes to use of Slack Services.

Transfers to other countries

Slack contractually warrants that it has no reason to believe that the laws and practices applicable to the processing of Personal Data by Slack or its Sub-Processors prevent Slack from fulfilling its obligations under its DPA or otherwise pose any materially different privacy risks as to inappropriate disclosure of Personal Data to foreign government law enforcement and intelligence agencies.

Safeguards in place to ensure an equivalent level of protection

This section helps Customers perform steps 4, 5 and 6 of the EDPB Transfer Impact Assessment:

Step 4: Adopt supplementary measures.

Step 5: Adopt necessary procedural steps.

Step 6: Re-evaluate.

This section summarizes the various contractual, technical and organizational measures that Slack makes available to ensure that an equivalent level of protection exists for European Personal Data subject to cross-border transfers by Customers in connection with their use of the Slack Services. In this section, we further explain why these measures ensure an equivalent level of protection and therefore allow for a lawful transfer of Personal Data outside of Europe using the Slack Services.

Please see the **Slack Security, Privacy and Architecture documentation, Security Practices and Security White Paper** for a more comprehensive overview of the measures in place to ensure the protection of Personal Data. We encourage our Customers to regularly re-evaluate the level of protection afforded to their data transferred to Third Countries.

Contractual safeguards

Standard contractual clauses

Slack has made available to all Customers the 2021 SCCs, which contain extensive protections around compelled disclosure and international data transfers. The 2021 SCCs were specifically drafted by the European Commission and approved by all EU member states subsequent to the Schrems II ruling in order to provide appropriate safeguards to allow for a lawful international transfer of personal data. This includes a warranty from Slack that it has no reason to believe that local laws applicable to Slack would prevent it from offering an adequate level of protection of Personal Data.

Contractual commitments

Slack has also offered extensive protections around compelled disclosure with respect to Customer Data in its DPA (see DPA section 7, “Government Access Requests”), and these protections are offered to all Customers globally (including when Customer Data stays within Europe). Slack strongly believes that these contractual protections provide Customers as much legal certainty as

possible in relation to compelled disclosure both within Europe and internationally.

As part of these contractual commitments:

- Slack will maintain appropriate measures to protect Personal Data in accordance with the requirements of data protection laws and regulations, including implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, national defense and public security.
- If Slack receives a request for data from a law enforcement or governmental entity determined to be valid, appropriate and legally binding, it will promptly notify the Customer (unless otherwise legally prohibited) so the Customer may seek legal remedies.
- To the extent that Slack is prohibited by law from providing such notification to the relevant Customer, Slack shall, when appropriate, seek to obtain a waiver of the prohibition to enable Slack to communicate as much information as possible, as soon as possible.
- Further, Slack commits to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful.
- Slack will pursue possibilities of appeal. When challenging a request, Slack commits to seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits.
- Slack will not disclose any data requested until required to do so under the applicable procedural rules.
- Slack also commits to provide the minimum amount of information permissible when responding to a request for disclosure based on a reasonable interpretation of the request.
- Slack will promptly notify the Customer if it becomes aware of any direct access by any law enforcement or governmental entity, and provide the Customer with available information, to the extent permitted by law.

Technical safeguards

Slack is committed to achieving and maintaining the trust of our Customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our Slack Services, including offering industry-leading technical measures to protect Personal Data against unauthorized access, as further described in this section.

An overview of the standard security controls applicable to the Slack Services is provided in the Slack **Security, Privacy and Architecture documentation**, **Security Practices** and **Security White Paper**. In addition, Slack offers a comprehensive set of security controls, as described below, that can help a Customer configure their Slack workspace in line with a Customer's own security standards.

Encryption

A key technical supplementary measure described in the EDPB Recommendations is encryption, including the management of encryption keys. Slack offers enhanced encryption services that Customers can leverage to protect their Customer Data.

Encryption in transit (default for all Slack plans)

The Slack Services use industry-accepted encryption products to protect Customer Data (1) during transmission between a Customer's network and the Slack Services, and (2) when at rest. The Slack Services support the latest recommended secure cipher suites and protocols to encrypt all traffic in transit.

All data transmitted between Slack clients and the Slack Service is done using strong encryption protocols. Slack supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption and SHA2 signatures, whenever supported by the clients. Slack encrypts all transfers of data to prevent the acquisition of such data by third parties, such as governmental authorities, who may gain physical access to the transmission mechanisms while the data is in transit. Slack only utilizes secure data transport via TLS 1.2 over HTTPS. This feature is always enabled to limit any third-party efforts to tamper with or tap into the data transfers between the two endpoints (Slack and our Customers).

Encryption at rest (default for all Slack plans)

Data at rest in Slack's production network is encrypted using FIPS 140-2 compliant encryption standards, which applies to all types of data at rest within Slack's systems—relational databases, file stores, database backups, etc. All encryption keys are stored in a secure server on a segregated network with very limited access. Slack has implemented appropriate safeguards to protect the creation, storage, retrieval and destruction of secrets such as encryption keys and service account credentials.

Enterprise key management (EKM may be purchased on enterprise grid plans)

With **Slack EKM**, organizations may use their own encryption keys—stored in Amazon's Key Management Service (AWS KMS)—to encrypt messages and files. EKM offers additional safeguards by creating an immutable audit log so that the Customer receives notification every time its data is accessed. The act of preserving or producing EKM content would trigger an observable entry in the access log available to the Customer. Customers may also revoke encryption keys to prevent access to unencrypted content.

Architecture and data segregation (default for all Slack Services):

The Slack Services are operated on a multi-tenant architecture at both the platform and infrastructure layers that is designed to segregate and restrict access to the data that Customers make available via the Slack Services, as more specifically

defined in your agreement with Slack (or its corporate affiliates) covering the use of the Slack Services ("Customer Data"), based on business needs. The architecture provides a logical data separation for each different customer via a unique ID.

Slack data residency ensures that sensitive Customer data is persisted only in the local region where the product is available.

Access controls:

It is important to note that as part of regular maintenance activities, Slack employees do not view Customer messages, channel names or any other content generated by users of the Slack Services. To minimize the risk of data exposure, Slack adheres to the principles of least privilege and role-based permissions when provisioning access—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities (see sections 2A and 2B above). All of our employees and contract personnel are bound to our policies regarding Customer Data, and we treat these issues as matters of the highest importance within our company. Please also review Slack's **Security Practices** and **Security White Paper** for more information.

Organizational safeguards

Slack has a number of organizational safeguards in place to protect personal data processed in the context of the Slack Services to ensure that the contractual commitments noted above are complied with in practice.

Data request policy

As part of our commitment to trust and transparency, our **Data Request Policy** outlines Slack's policies and procedures for responding to requests from government and law enforcement entities. This policy guides our practices with respect to requests for third-party data, requests by legal authorities, customer notice and international requests for data. Slack only provides data in response to legally binding, jurisdictionally appropriate and valid legal processes. In addition, a legal process must be jurisdictionally appropriate to the data sought, including data stored through Slack's **data residency feature**.

Transparency report

Our annual **Transparency Report** details requests for data that we've received, including those from law enforcement and government entities. As further explained in Slack's **Data Request Overview**, Slack does not and cannot be ordered to take any action to facilitate bulk surveillance as contemplated in Executive Order 12333, nor is Slack eligible to receive a request under FISA § 702 for "upstream" surveillance (the type of order principally addressed in, and deemed problematic by, the Schrems II decision).

For more information on Slack's privacy program and our commitment to protecting the security and privacy of your data, please visit our **Trust Center**.

Internal policies

Slack has internal policies, including globally applicable standards and processes, that govern our approach to responding to

requests to access Personal Data from governments. Regardless of the type of data, and the type of legal process issued, any and all requests for data at Slack are overseen by a dedicated group of professionals. A small group of employees have visibility into Slack's legal process tracking and production pipelines and determine the accuracy, validity and appropriateness of requests in consultation with outside counsel. Requests from law enforcement for data stored through Slack's **data residency feature** must be jurisdictionally appropriate to the data sought and are handled by a small number of personnel within Slack Ltd. (Ireland).

Slack determines equivalent protection of personal data

As outlined above, when assessing potential data protection risks in relation to compelled disclosure and international data transfers post-Schrems II, the GDPR requires that data importers and data exporters should take into account the specific circumstances of the transfer and any safeguards put in place (including relevant contractual, technical and organizational measures applying to the Personal Data). In other words, a holistic approach is required in which the entire array of contractual, technical and organizational security measures offered by Slack and those that can be implemented by Customers need to be considered so that an appropriate risk assessment can be made. The GDPR does not require that organizations eliminate all risk, which would be impossible, but to take appropriate measures to mitigate risks.

Taking into account the information set out in this document, Customers can use Slack Services to transfer their data outside of Europe in compliance with European law by relying on the industry-leading contractual, technical and organizational frameworks described in this document.

About Slack

Slack makes work simpler, more pleasant and more productive. It's a channel-based messaging platform for the enterprise that brings the right people, information and tools together to get work done.

From FTSE 100 companies to corner shops, millions of people around the world use Slack to connect their teams, unify their systems and drive their business forward.

This document is provided for informational purposes. It is not intended to provide legal advice. Slack urges its customers to consult with their own legal counsel to familiarize themselves with the requirements that govern their specific situations. This information is provided as of the date of document publication and may not account for changes after the date of publication.