SWEETHAWK

DATA TRANSFER IMPACT ASSESSMENT

Introduction

We have prepared this data transfer impact assessment document (**TIA**) in order to provide SweetHawk customers (**you**) with information in respect of the transfer of data when using any of our applications acquired through our website located at https://sweethawk.co/zendesk or www.zendesk.com/apps (**Application**) to enable you to conduct a data transfer impact assessment. This TIA is prepared in relation to the "Schrems II" ruling of the Court of Justice for the European Union and the recommendations from the European Data Protection Board.

Furthermore, this TIA describes the legal requirements SweetHawk follows regarding transfers of your personal information and data from the European Economic Area to the United States of America and our ability to comply with our obligations as data importer under the Standard Contractual Clauses (**SCCs**).

1. Know your international data transfers from the EU

Where we process personal data which is governed by European data protection laws as a data processor on your behalf, we comply with our obligations as set out in our Privacy Policy and Data Processing Addendum (**DPA**). Our DPA includes the SCCs and the following:

- Details of how we process customer personal data; and
- Details of our security measures.

You may refer to our DPA for further information regarding our processing activities, the types of customer personal data we process and transfer and the categories of data subjects.

A list of our authorised sub-processors, as updated from time-to-time, is specified here https://sweethawk.com/dpa.

We may transfer customer personal data wherever we or our third-party service providers operate for the purpose of providing you the Application.

Your personal data will be stored on our servers which are located in the United States of America and processed in the United States of America and Australia.

2. Identify the transfer tools relied upon

If personal data from the European Economic Area is transferred to us, we rely upon the SCCs to provide an appropriate safeguard for the transfer. The SCCs are specified in our DPA which is available here: https://sweethawk.com/dpa.

If your personal data is from the European Economic Area is transferred between SweetHawk group companies or transferred by SweetHawk to third-party sub-processors, we request our sub-processors execute a DPA to ensure that we are GDPR compliant.

3. Consider whether laws or practices in the receiving country impact the effectiveness of the transfer tools relied on

U.S. Surveillance Laws

The following US laws were identified by the Court of Justice of the European Union in Schrems II as being potential obstacles to ensuring essentially equivalent protection for personal data in the US:

Section 702 of the Foreign Intelligence Surveillance Act (**FISA 702**)

This legislation allows US government authorities to compel disclosure of information about non-US persons located outside the US for the purposes of foreign intelligence information gathering.

In order to gather the information, it must be approved by the Foreign Intelligence Surveillance Court in Washington DC.

Remote computing service providers can be included within the scope of this legislation.

Executive Order 12333 (**EO 12333**)

The EO 12333 enables US intelligence agencies to conduct surveillance outside of the US as it allows US intelligence agencies to collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means. This may include accessing underwater cables carrying internet data in transit to the US. EO 12333 does not rely on the cooperation of service providers to provide information to it, rather it relies on exploiting vulnerabilities in telecommunications infrastructure.

Further information on the US surveillance legislation and the relevance to computer service providers and the SCCs can be found here in the whitepaper published by the US government.

In respect of FISA 702, the whitepaper specifies that for most companies the concerns about national security access to company data highlighted by Schrems II are “unlikely to arise because the data they handle is of no interest to the U.S. intelligence community”. Companies handling “ordinary commercial information such as employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data.”

If there are violations for FISA 702, there may be actions you can take if the measures from the Schrems II ruling are not followed, such as compensation and damages.

In respect EO 12333, the whitepaper states that this order does not simply “authorise the U.S. government to require any company or person to disclose data.” Instead, EO 12333 must rely on a statute, such as FISA 702 in order to collect data. The type of data which was collected in Schrems II was a bulk data collection, such data collection is expressly prohibited under EO 12333.

Clarifying Lawful Overseas Use of Data Act (**Cloud Act**)

The CLOUD Act only permits U.S. government access to data in criminal investigations after obtaining a warrant approved by an independent court based on probable cause of a specific criminal act. The CLOUD Act does not allow U.S. government access in national security investigations, and it does not permit bulk surveillance.

Are we subject to FISA 702 or EO 12333?

Strictly speaking, as we are a SaaS company with service providers in the US, we could be subject to FISA 702 if it can be established that we are a remote computer service provider. However, we do not process personal data which is likely to be subject to an investigation or under surveillance of US intelligence agencies.

Historically, US government agencies has applied FISA 702 to target market providers that have traffic flowing through their internet backbone and that carry traffic for third parties (such as telecommunications carriers). As we do not provide internet backbone services and only process personal data of our own customers, it is unlikely we will be subject to a surveillance order under FISA 702.

EO 12333 does not compel private companies such as us to disclose personal data to US government agencies unless an independent US court has authorised a specific type of foreign intelligence data request, which is generally not related to commercial information.

We do not voluntarily provide personal data to US government agencies and will only comply with a request if compelled by law.

Have we ever received a personal data request from a US government agency?

We have never received a request from a US government agency under FISA 702 or EO 12333 in connection with personal data.

While we may be subject to US surveillance requests identified in Schrems II, we have not yet been requested to provide any such information and we are unlikely to be contacted by any US government agencies in respect of the personal data we process.

4. **Adopt supplementary procedures (such as contractual, technical or organisational measures) that provide an equivalent level of protection to data transfers**

Technical Measures

We take appropriate technical and security measures to protect against unauthorised access to or unauthorised alteration, disclosure or destruction of data. These measures may include internal reviews of our data collection, storage and processing practices and security measures, including appropriate encryption and ensuring our data processor maintains an adequate level of data protection and physical security measures to guard against unauthorised access to systems where we store personal data.

Contractual Measures

Furthermore, we are obliged contractually to adopt suitable technical and organisational processes to keep your personal data safe and secure, as set out in the SCCs in our DPA, which we enter into with our customers and suppliers. We also require our subprocessors to sign a DPA which includes the SCCs.

In respect of government access to personal data, under the SCCs we are obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

Organisational Measures

We will only share your personal data with our service providers who have been qualified by us through our due diligence process and subject matter experts, to ensure your personal data received adequate protection.

We also take into account the associated level of risk, the service provider's security policies, measures, and third party audits, and whether the security provider has a mature privacy program that respects the rights of data subjects.

We adopt a privacy by design approach to handling your personal data in accordance with our Privacy Policy, available here: https://sweethawk.com/privacy.

In addition, all of our employees are informed about their obligations in respect of handling personal data and their obligations under the SCCs.

5. Take the procedural steps required to implement the supplementary measures

Given the personal data we collect, the nature of the services we provide and our technical, organisational and contractual measures, we do not consider that the risks involved in transferring and processing personal data from the European Economic Area to the United States of America prevent us from complying with our obligations as a data importer under the SCCs or to ensure your personal data and rights remain protected.

6. Monitor and re-evaluate at appropriate intervals

We will review and consider the risks involved with the transfer of personal data and evaluate the measures we have taken to address changes to data privacy regulations and risk environments associated with transfers of personal data outside of the European Economic Area.