Last Updated: 24 November 2022

Data Transfer Impact Assessment

OVERVIEW

This document provides information to help Probax customers conduct data transfer impact assessments in connection with their use of Probax products and services, in light of the "Schrems II" ruling of the Court of Justice for the European Union and the recommendations from the European Data Protection Board.

In particular, this document describes the legal regimes applicable to Probax in the US, the safeguards Probax puts in place in connection with transfers of customer personal data from the European Economic Area, United Kingdom or Switzerland ("Europe"), and Probax's ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

STEP 1: KNOW YOUR TRANSFER

Where Probax processes personal data governed by European data protection laws as a data processor (on behalf of our customers), Probax complies with its obligations under its Customer Data Processing Addendum ("DPA") available here.

Please refer to Exhibit A of the DPA for information on the nature of Probax's processing activities in connection with the provision of the Services, the types of customer personal data we process and transfer, and the categories of data subjects.

A list of all of our data subprocessors is available here.

We may transfer customer personal data wherever we or our third-party service providers operate for the purpose of providing you the Services. The locations will depend on the particular Probax Services you use, as outlined in the table below.

Product(s) and Services	In what countries does Probax store Customer Personal Data?	In what countries does Probax process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
Hive	United States	Australia, Germany, Singapore, United Kingdom, United States
Scout	N/A (Scout only transfers data to hive)	Wherever the Scout agent is installed will transfer to Probax's Datacenter in the United States.

Product(s) and Services	In what countries does Probax store Customer Personal Data?	In what countries does Probax process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
Honeycomb Storage (Hot/Cold/Object)	Asia-Pacific, Europe (EEA), United Kingdom, United States **Note:** Storage location (country) is chosen by the Customer.	Data is transferred from wherever the customer is physically located to whichever Probax datacenter they choose. No data is transferred to any other region than what the customer requests.
Second Colony DRaaS	Australia, United States **Note:** Storage location (country) is chosen by the Customer.	Data is transferred from wherever the customer is physically located to whichever Probax datacenter they choose. No data is transferred to any other region than what the customer requests.
Microsoft 365 Backup & Archive	Australia, United Kingdom, United States **Note:** Storage location (country) is chosen by the Customer.	Data is transferred from wherever the customer is physically located to whichever Probax datacenter they choose. No data is transferred to any other region than what the customer requests.
Dropbox Backup & Archive	United States, United Kingdom **Note:** Storage location (country) is chosen by the Customer.	Data is transferred from wherever the customer is physically located to whichever Probax datacenter they choose. No data is transferred to any other region than what the customer requests.

STEP 2: IDENTIFY THE TRANSFER TOOL RELIED UPON

Where personal data originating from Europe is transferred to Probax, Probax relies upon the European Commission's SCCs to provide an appropriate safeguard for the transfer. Probax's Customer Data Processing Addendum ("DPA") is available here.

Where customer personal data originating from Europe is transferred between Probax group companies or transferred by Probax to third-party subprocessors, Probax enters into SCCs with those parties.

STEP 3: ASSESS WHETHER THE TRANSFER TOOL RELIED UPON IS EFFECTIVE IN LIGHT OF THE CIRCUMSTANCES OF THE TRANSFER

FISA 702 and Executive Order 12333 (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:

- FISA Section 702 ("FISA 702") – 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. This information gathering must be approved by the Foreign Intelligence Surveillance Court in Washington, DC. In-scope providers subject FISA 702 are electronic communication service providers ("ECSP") within the meaning of 50 U.S.C § 1881(b)(4), which can include remote computing service providers ("RCSP"), as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711.
- Executive Order 12333 ("EO 12333") - authorizes intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. In particular, it provides authority for 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 compelled assistance of service providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure.

Further information about these US surveillance laws can be found in the U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after Schrems II whitepaper from September 2020. This whitepaper details the limits and safeguards pertaining to US public authority access to data and was issued in response to the Schrems II ruling.

Regarding FISA 702 the whitepaper notes:

- For most companies in Europe (EEA), the concerns about national security access to company data highlighted by Schrems II are unlikely to arise because:
    1. Probax is an Australian-owned company.
    2. Company data that relates to data protection backups, archives and replicas are all stored in a geographic region chosen by the customer. For companies in Europe (EEA), all data protection data will reside within Europe.
    3. All other 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 like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data."

- There is individual redress, including for EU citizens, for violations of FISA section 702 through measures not addressed by the court in the Schrems II ruling, including FISA provisions allowing private actions for compensatory and punitive damages.

Regarding Executive Order 12333 the whitepaper notes:

- EO 12333 does not on its own "authorize 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 to collect data.
- Bulk data collection, the type of data collection at issue in Schrems II, is expressly prohibited under EO 12333.

Is Probax subject to FISA 702 or EO 12333?

Australian-owned companies may be subject to surveillance under FISA 702 if the company is believed to be involved in activities that threaten the national security of the United States. Additionally, if the company operates in the US or is involved in activities that involve US citizens, it may be subject to surveillance under Executive Order 12333. However, the specific circumstances of the company would need to be evaluated to determine whether surveillance is warranted and if the company would be subject to surveillance under these laws. However, Probax does not process personal data that is likely to be of interest to US intelligence agencies.

Furthermore, Probax is not likely to be subject to upstream surveillance orders under FISA 702, the type of order principally addressed in, and deemed problematic by, the Schrems II decision. Probax does not provide internet backbone services, but instead only carries traffic involving its own customers. To date, the U.S. Government has interpreted and applied FISA 702 upstream orders to only target market providers that have traffic flowing through their internet backbone and that carry traffic for third parties (i.e., telecommunications carriers).

EO 12333 contains no authorization to compel private companies (such as Probax) to disclose personal data to US authorities and FISA 702 requires an independent court to authorize a specific type of foreign intelligence data acquisition which is generally unrelated to commercial information. In the unlikely event that US intelligence agencies were interested in the type of data that Probax processes, safeguards such as the requirement for authorization by an independent court and the necessity and proportionality requirements would protect data from excessive surveillance.

What is Probax's practical experience dealing with government access requests?

To date, Probax has never received a US National Security Request (including requests for access under FISA 702 or direct access under EO 12333) in connection with customer personal data.

Therefore, while Probax may technically be subject to the surveillance laws identified in Schrems II, we have not been subject to these types of requests in our day-to-day business operations.

STEP 4: IDENTIFY THE TECHNICAL, CONTRACTUAL AND ORGANIZATIONAL MEASURES APPLIED TO PROTECT THE TRANSFERRED DATA

Probax provides the following technical measures to secure data:

- **Data residency:** Probax allows customers to pin in-scope product content at rest to a location.
- **Encryption:** Probax offers data encryption at rest and in transit.
- **Security and certifications:** We have a formal security management program, and we review our Information Security Management Program (ISMP) on an annual basis. Additional information about Probax's security practices and certifications are available here.

Probax's contractual measures are set out in our Data Processing Agreement which incorporates the SCCs. In particular, we are subject to the following requirements:

- **Technical measures:** Probax is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data (both under the Customer DPA as well as the SCCs we enter into with customers, service providers, and between entities within the Probax group).
- **Transparency:** Probax is obligated under the SCCs to notify its customers in the event it is made subject to a request for government access to customer personal data from a government authority. In the event that Probax is legally prohibited from making such a disclosure, Probax is contractually obligated to challenge such prohibition and seek a waiver.
- **Actions to challenge access:** Under the SCCs, Probax is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

Probax's organizational measures to secure data include:

- **Policy for government access:** To obtain data from Probax, law enforcement officials must provide legal process appropriate for the type of information sought, such as a subpoena, court order, or a warrant.
- **Onward transfers:** Whenever we share your data with Probax service providers, we remain accountable to you for how it is used. We require all service providers to undergo a thorough cross-functional diligence process by subject matter experts in our Security, Privacy, and Risk & Compliance Teams to ensure our customers personal data receives adequate protection. This process includes a review of the data Probax plans to share with the service provider and the associated level of risk, the supplier's security policies, measures, and third party audits, and whether the supplier has a mature privacy program that respects the rights of data subjects. We provide a list of our sub-processors on our subprocessors page.
- **Employee training:** Probax provides regular data protection training to all Probax staff, as per Probax's security practices and certifications.

STEP 5: PROCEDURAL STEPS NECESSARY TO IMPLEMENT EFFECTIVE SUPPLEMENTARY MEASURES

In light of the information provided in this document, including Probax's practical experience dealing with government requests and the technical, contractual, and organizational measures Probax has implemented to protect customer personal data, Probax considers that the risks involved in transferring and processing European personal data in/to the US and AU do not impinge on our ability to comply with our obligations under the SCCs (as "data importer") or to ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time.

STEP 6: RE-EVALUATE AT APPROPRIATE INTERVALS

Probax will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data outside of Europe.