Data Transfer Impact Assessment

Overview

This assessment provides information to help OwnBackup customers conduct data transfer impact assessments in connection with their use of OwnBackup products, in light of the recommendations from the European Data Protection Board after the “Schrems II” ruling by the Court of Justice for the European Union.

Specifically, this page describes the legal schemas applicable to OwnBackup in the United States, the safeguards OwnBackup puts in place in connection with transfers of Customer Data from the European Economic Area, the United Kingdom or Switzerland ("Europe"), and OwnBackup's ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

For more details about OwnBackup’s broader privacy position, including access to our Data Processing Addendum (“DPA”), visit this page.

Step 1: Know your transfer

OwnBackup maintains detailed records of processing and has clearly identified the instances where transfers occur.

Where OwnBackup processes personal data governed by the data protection laws and regulations of Europe as a data processor (on behalf of our customers as data controllers), OwnBackup complies with its obligations under its DPA. The OwnBackup DPA incorporates the SCCs and provides the following information:

- identification of the subprocessors applicable to OwnBackup’s processing at the time the DPA is executed (Schedule 1)
- description of processing of customer personal data based on the typical use-case of our customers (Schedule 3); and
- description of OwnBackup’s security measures (Schedule 4)

Please refer to Schedule 3 of the DPA for information on the nature of OwnBackup's processing activities in connection with the provision of OwnBackup’s applications, as well as the categories of data subjects and the types of customer personal data we typically process and transfer.

We may transfer customer personal data wherever we or our third-party subprocessors operate, strictly for the purpose of providing our SaaS applications to our customers. The transfer locations will depend on the particular OwnBackup applications a customer is using and the locations where the customer chooses to deploy the applications, as further outlined in the DPA.

Step 2: Identify the transfer tool relied upon

Where personal data originating from Europe is transferred to OwnBackup in the U.S., OwnBackup relies upon the European Commission's SCCs to provide an appropriate safeguard for the transfer as supplemented or amended as required by data protection authorities. To review OwnBackup's DPA (which incorporates the SCCs) please visit this page.

For the sake of completeness, where personal data originating from Europe is transferred to OwnBackup in Israel, OwnBackup relies on Israel's adequacy decision.

Step 3: Assess whether the transfer tool relied upon is effective in light of the circumstances of the transfer

Identifying applicable U.S. Surveillance Laws

A) FISA 702 and Executive Order 12333

The following U.S. 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 U.S.:

- ***FISA Section 702 ("FISA 702")*** This allows U.S. government authorities to compel disclosure of information about non-U.S. persons located outside the U.S. for the purposes of gathering foreign intelligence information. Such 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 services ("RCS"), as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711.

- ***Executive Order 12333 ("EO 12333")*** This authorizes intelligence agencies (like the U.S. National Security Agency) to conduct surveillance outside of the U.S., providing authority for U.S. intelligence agencies to collect foreign "signals intelligence" information. This is information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means, potentially including accessing underwater cables which carries internet data in transit to the U.S. EO 12333 does not rely on the compelled assistance of subprocessors, appearing instead to rely on exploiting vulnerabilities in telecommunications infrastructure.

The U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II whitepaper, published by the U.S. Department of Commerce in September 2020 in response to the Schrems II ruling, provides useful information about these laws. This whitepaper details the limits and safeguards pertaining to U.S. public authority access to data.

Regarding FISA 702 it notes:

- 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 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 it 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.

B) CLOUD Act

For more information on the CLOUD Act, review What is the CLOUD Act? by BSA Software Alliance outlining the scope of the CLOUD Act.

The document notes that the 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; and

- does not allow U.S. government access in national security investigations, and it does not permit bulk surveillance

Is OwnBackup subject to FISA 702 or EO 12333?

OwnBackup, like most U.S.-based SaaS companies, could technically be subject to FISA 702 where it is deemed to be an electronic communication service provider (ECSP). However, OwnBackup does not process personal data that is likely to be of interest to U.S. intelligence agencies.

Furthermore, OwnBackup 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. OwnBackup 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 OwnBackup) to disclose personal data to U.S. 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 event that U.S. intelligence agencies were interested in the type of data that OwnBackup 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 OwnBackup's practical experience dealing with government access requests?

As of the date set out below, OwnBackup has never received a U.S. National Security Request (including requests for access under FISA 702 or direct access under EO 12333) in connection with customer personal data.

Therefore, while OwnBackup may technically be subject to the surveillance laws identified above we have not been subject to these types of requests in our day-to-day business operations and, for the reasons identified on this page, we believe it is unlikely we will be subject to them in the future.

Step 4: Identify the technical, contractual and organizational measures applied to protect the transferred data

OwnBackup provides the following technical measures to secure customer data:

- Data residency: OwnBackup’s customers choose the hosting location for the deployment of the OwnBackup applications and OwnBackup will never transfer customer’s data from the select locations without customer’s consent.

- Encryption: OwnBackup offers data encryption at rest and in transit, and we also provide options that allow our customers to manage their own encryption keys within the OwnBackup applications.

- Security and certifications: Additional information about OwnBackup's security practices and certifications are available in Schedule 4 of the DPA, and on our Trust site.

OwnBackup's contractual measures are set out in our DPA which incorporates the SCCs. In particular, we are subject to the following requirements:

- Technical measures: OwnBackup is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data (both under the DPA as well as the SCCs we enter into with customers, subprocessors, and between entities with the OwnBackup group).
- Transparency: OwnBackup 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 OwnBackup is legally prohibited from making such a disclosure, OwnBackup is contractually obligated to provide only that information which it is required by law to provide.
- Actions to challenge access: Under the SCCs, OwnBackup is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

OwnBackup's organizational measures to secure customer data include:

- Policy for government access: OwnBackup publishes and follows its Principles for Government Requests for Data in responding to any government requests for data. To obtain data from OwnBackup, law enforcement officials must provide legal process appropriate for the type of information sought, such as a subpoena, court order, or a warrant. OwnBackup will never produce customer personal data to a requesting government agency on a voluntary basis.

- Onward transfers: Whenever we share a customer's data with OwnBackup subprocessors, we remain accountable to the customer for how it is used. We require all subprocessors to undergo a thorough due diligence process by subject matter experts in our Security, Privacy, and Legal Teams to ensure our customers' personal data receives adequate protection. This process includes a review of the data OwnBackup plans to share with the subprocessor 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 website.

- Employee training: OwnBackup provides data protection training to all OwnBackup staff who may access customer personal data within our applications.

Step 5: Procedural steps necessary to implement effective supplementary measures

In light of the information provided in this document, and the technical, contractual, and organizational measures OwnBackup has implemented to protect customer personal data, OwnBackup considers that the risks involved in transferring and processing European personal data in/to the U.S. with respect to our applications do not impinge on our ability to comply with our obligations under the SCCs (as "data importer") and to ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time.

Step 6: Re-evaluate at appropriate intervals

OwnBackup monitors the legal regime of the U.S. on an on-going basis and will re-evaluate any risks which may impact transfers of personal data outside of Europe and the measures it has implemented to address changing data privacy regulations and risk environments associated with such transfers.

Last update October 17, 2022

***Legal Notice**: This document: (a) is for informational purposes only, (b) represents current OwnBackup application offerings and practices, which are subject to change without notice, (c) does not create any commitments or assurances from OwnBackup and its affiliates, suppliers or licensors, and (d) does not constitute legal advice. The responsibilities and liabilities of OwnBackup to its customers are controlled by OwnBackup agreements, and this document is not part of, nor does it modify, any agreement between OwnBackup and its customers. This document is not a substitute for an OwnBackup customer's own legal analysis.*