Rhapsody's Data Transfer Impact Assessment Guide for Customers

Last updated on: March 31, 2023

OVERVIEW

This document provides information to help Rhapsody customers conduct data transfer impact assessments in connection with their use of Rhapsody products, 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 Rhapsody in the US, the safeguards Rhapsody puts in place in connection with transfers of customer personal data from the European Economic Area, United Kingdom or Switzerland ("Europe"), and Rhapsody's ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

For more details about Rhapsody's GDPR compliance program please visit this Rhapsody Data Privacy and Security page.

STEP 1: KNOW YOUR TRANSFER

Where Rhapsody processes personal data governed by European data protection laws as a data processor (on behalf of our customers), Rhapsody complies with its obligations under its GDPR Addendum: Data Protection and Security available at the link above ("GDPR DPA Addendum"). The Rhapsody Data Privacy and Security page, linked above, incorporates a description of Rhapsody's processing of customer personal data. For additional information on Rhapsody security measures see Step 4*, Identify the technical, contractual, and organizational measures applied to protect the transferred data*, below.

Please refer to the Rhapsody Data Privacy and Security page for information on the nature of Rhapsody'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 Rhapsody's data subprocessors is available on the Rhapsody Data Privacy and Security page.

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 Rhapsody Services you use, as outlined in the chart below.

Product(s) and Services	**In what countries does Rhapsody store Customer Personal Data?**	**In what countries does Rhapsody process (e.g., access, transfer, or otherwise handle) Customer Personal Data?**
Rhapsody Support in the UK or EU	United States, European Union, United Kingdom	United States, United Kingdom, European Union, New Zealand, Philippines, Australia.
Rhapsody Professional Services in the UK or EU	United States, European Union, United Kingdom	United States, United Kingdom, European Union.
Rhapsody Development	United States, Denmark, New Zealand	United States, Denmark, New Zealand.

STEP 2: IDENTIFY THE TRANSFER TOOL RELIED UPON

Where personal data originating from Europe is transferred to Rhapsody, Rhapsody relies upon the European Commission's SCCs to provide an appropriate safeguard for the transfer. To review Rhapsody's GDPR DPA Addendum (which incorporates the SCCs) please visit the Rhapsody Data Privacy and Security page.

Where customer personal data originating from Europe is transferred between Rhapsody group companies or transferred by Rhapsody to third- party subprocessors, Rhapsody 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

Is Rhapsody subject to US Surveillance laws?

Rhapsody, like most US-based SaaS companies, could technically be subject to FISA Section 702 where it is deemed to be a remote computing service providers ("RCSP") as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711. However, Rhapsody does not process personal data that is likely to be of interest to US intelligence agencies.

Furthermore, Rhapsody 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. Rhapsody 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). 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."

Executive Order 12333 contains no authorization to compel private companies (such as Rhapsody) 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 event that US intelligence agencies were interested in the type of data that Rhapsody processes, safeguards such as the requirement for authorization by an independent court and the necessity and proportionality requirements would protect data from excessive surveillance.

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.

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

To date, Rhapsody 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 Rhapsody 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

Rhapsody provides the following to secure customer data:

- **Technical measures**
  - Secure and hardened operating systems are in place
  - Data is encrypted in transit and at rest
  - Role-based access controls (RBAC) follow the Least Privilege Principle
  - All systems with access to customer data are monitored for anomalous security events 24x7 (SIEM)

- Comprehensive audit logging is implemented
- Governance and incident management procedures including Root Cause Analysis (RCA) are in use
- Routine third party penetration testing is conducted
- Industry leading anti-virus technologies are implemented

- **Data residency**: Rhapsody allows customers to pick where their Rhapsody-hosted instance of software will be located from a list of where the subprocessors have data centers.
- **Security and certifications**: Additional information about Rhapsody's security practices and certifications are available on Rhapsody Data Privacy and Security webpage.

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

- **Technical measures:** Rhapsody is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data (both under the Data Processing Addendum as well as the SCCs we enter into with customers, service providers, and between entities within the Rhapsody group).
- **Transparency:** Rhapsody 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 Rhapsody is legally prohibited from making such a disclosure, Rhapsody is contractually obligated to challenge such prohibition and seek a waiver.
- **Actions to challenge access:** Under the SCCs, Rhapsody is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

Rhapsody's **organizational measures** to secure customer data include:

- **Policy for government access**: To obtain data from Rhapsody, law enforcement officials must provide a 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 Rhapsody 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 & Compliance Teams to ensure our customers' personal data receives adequate protection. This process includes a review of the data Rhapsody 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 Rhapsody Privacy and Security page.

- **Privacy by design**: Rhapsody's Privacy Principles outline Rhapsody's global approach to privacy and take into account administrative, technical, and physical safeguards required to protect all types of data including personal data and protected health information.
- **Employee training:** Rhapsody provides data protection training to all Rhapsody staff annually.

STEP 5: PROCEDURAL STEPS NECESSARY TO IMPLEMENT EFFECTIVE SUPPLEMENTARY MEASURES

In light of the information provided in this document, including Rhapsody's practical experience dealing with government requests and the technical, contractual, and organizational measures Rhapsody has implemented to protect customer personal data, Rhapsody considers that the risks involved in transferring and processing European personal data in/to the US 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

Rhapsody 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.

Legal Notice: Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Rhapsody product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Rhapsody and its affiliates, suppliers, or licensors. The responsibilities and liabilities of Rhapsody to its customers are controlled by Rhapsody agreements, and this document is not part of, nor does it modify, any agreement between Rhapsody and its customers.