

Atlassian's Data Transfer Impact Assessment Guide for Customers

Last updated on: 23 Sep 2021

Overview

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

For more details about Atlassian’s GDPR compliance program please visit [this page](#).

Step 1: Know your transfer

Where Atlassian processes personal data governed by European data protection laws as a data processor (on behalf of our customers), Atlassian complies with its obligations under its Data Processing Addendum available on this [page](#). The Atlassian DPA incorporates the SCCs and provides the following information:

- description of Atlassian’s processing of customer personal data (Exhibit A); and
- description of Atlassian’s security measures (Exhibit B)

Please refer to Exhibit A to the DPA for information on the nature of Atlassian’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 and an RSS feed subscription where you can stay up-to-date on changes 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 Atlassian Services you use, as outlined in the chart below.

Product(s) and Services	In what countries does Atlassian store Customer Personal Data?	In what countries does Atlassian process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
Atlassian cloud account profile (Identity)	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Jira and Confluence Cloud	Asia-Pacific, Europe (EEA), United States	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States.
Jira Service Management / Jira Work Management	Global, Europe (EEA), United States	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States.
Bitbucket Cloud	United States, Europe (EEA), Canada, Asia-Pacific	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States
Compass	Asia-Pacific, Europe (EEA), United States	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States.
Trello	Asia-Pacific, Canada, Europe (EEA), Global, United States	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States

Opsgenie	Europe (EEA), Global, United States	Australia, Brazil, Netherlands, Philippines, Turkey, United Kingdom, United States
Statuspage	United States	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States
Jira Align	United States, Asia-Pacific, Europe (EEA)	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States
Halp	United States	United States
Atlassian business operations and analytics ("Usage Data")	United States	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States
Atlassian support	Asia-Pacific, Canada, Europe (EEA), United States	Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, Ukraine, United Kingdom, United States

Step 2: Identify the transfer tool relied upon

Where personal data originating from Europe is transferred to Atlassian, Atlassian relies upon the European Commission's SCCs to provide an appropriate safeguard for the transfer. To review Atlassian's Data Processing Addendum (which incorporates the SCCs) please visit this [page](#).

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

U.S. Surveillance Laws

FISA 702 and Executive Order 12333

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 to 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, 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 EO 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.

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 whitepaper notes:

- 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.

Is Atlassian subject to FISA 702 or EO 12333?

Atlassian, like most US-based SaaS companies, could technically be subject to FISA 702 where it is deemed to be a RCSP. However, Atlassian does not process personal data that is likely to be of interest to US intelligence agencies.

Furthermore, Atlassian 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. Atlassian 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 Atlassian) 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 Atlassian 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 Atlassian's practical experience dealing with government access requests?

Atlassian publishes an annual [Transparency Report](#) with information about government requests to access data. To date, Atlassian 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 Atlassian 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

Atlassian provides the following **technical measures** to secure customer data:

- **Data residency:** Atlassian allows customers to [pin in-scope product content at rest to a location](#). Planned expansions to our data residency program (including data residency for apps and additional locations) are highlighted in Atlassian's [cloud roadmap](#)
- **Encryption:** Atlassian offers data [encryption at rest and in transit](#), and we are building [BYOK encryption](#) as highlighted in Atlassian's [cloud roadmap](#)
- **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 Atlassian's security practices and certifications are available in Exhibit B of the [Data Processing Addendum](#), and on our [Trust site](#).

Atlassian's **contractual measures** are set out in our [Data Processing Addendum](#) which incorporates the SCCs. In particular, we are subject to the following requirements:

- **Technical measures:** Atlassian 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 with the Atlassian group).
- **Transparency:** Atlassian 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 Atlassian is legally prohibited from making such a disclosure, Atlassian is contractually obligated to challenge such prohibition and seek a waiver.
- **Actions to challenge access:** Under the SCCs, Atlassian is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

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

- **Policy for government access:** Atlassian publishes and follows [Atlassian Guidelines for Law Enforcement Requests](#) in responding to any government requests for data. To obtain data from Atlassian, 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 Atlassian 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 Atlassian 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](#) (subscribe to our RSS feed so you can stay up-to-date on any changes).

- **Privacy by design:** Atlassian's [Privacy Principles](#) outline Atlassian's approach to privacy, and more detailed information on privacy in our machine learning intelligent experiences is available [here](#).
- **Employee training:** Atlassian provides data protection training to all Atlassian staff.

Step 5: Procedural steps necessary to implement effective supplementary measures

In light of the information provided in this document, including Atlassian's practical experience dealing with government requests and the technical, contractual, and organizational measures Atlassian has implemented to protect customer personal data, Atlassian 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

Atlassian 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 Atlassian product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Atlassian and its affiliates, suppliers, or licensors. The responsibilities and liabilities of Atlassian to its customers are controlled by Atlassian agreements, and this document is not part of, nor does it modify, any agreement between Atlassian and its customers.