CIBT

Newland Chase
A CIBT COMPANY

CIBTvisas

Newland Chase
Education
A CIBT COMPANY

BLAIR
A CIBT COMPANY

CIBT Data Transfer Impact Assessment

Last updated on: February 26, 2024

Overview

This document provides information to help CIBT customers conduct data transfer impact assessments in connection with their use of CIBT 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.

This document describes the legal regimes applicable to CIBT in the USA, the safeguards CIBT puts in place in connection with transfers of customer personal data from the European Economic Area, United Kingdom or Switzerland ("Europe") – as well as other locations with similar controls - and CIBT's ability to comply with its obligations as a "data importer".

Where CIBT processes personal data governed by either UK or European data protection laws (or other locations with similar protection laws) as a data processor (on behalf of our customers), CIBT complies with its obligations under its Data Processing Addendum. The CIBT DPA provides the following information:

- description of CIBT’s processing of customer personal data, and
- description of CIBT’s security measures

A DPA is available upon request that contains more information on the nature of CIBT'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 our data sub processors is available here and covers the countries in scope for your services.

We may transfer customer personal data wherever we or our third-party service providers operate for the purpose of providing you with the Services. The location(s) will depend on the CIBT Services you use, as outlined in the chart below.

Product(s) and Services	**In what countries does CIBT store Customer Personal Data?**	**In what countries does CIBT process (e.g., access, transfer, or otherwise handle) Customer Personal Data?**
CIBT and Newland Chase account profile (Identity)	Germany (primary), United States, Switzerland, Australia, England, and Ireland.	Depending on the country of destination, this could be any country. (Embassies are foreign land).
Service Management CIBT	Germany, United States, Switzerland, Australia, England, and Ireland	Processing offices are in Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, Hong Kong, India, Ireland, Mexico, Netherlands, Norway, Singapore, South Africa, Spain, Sweden, Switzerland, United Kingdom, and the United States. Depending on the destination, this could be any country (Embassies are foreign land).

Product(s) and Services	In what countries does CIBT store Customer Personal Data?	In what countries does CIBT process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
Service Management Newland Chase	Germany (primary), United States, Switzerland, Australia, England, and Ireland.	Processing offices are in Argentina, Australia, Brazil, Canada, China, Germany, India, Japan, Mexico, Netherlands, Singapore, Spain, Switzerland, United Arab Emirates, United Kingdom, United States. Depending on the destination, this could be any country (Embassies are foreign land).
Service Management Blair Consular Services	England	UK and Ireland.
CIBT business operations and analytics (“Usage Data”)	Germany (primary), United States, Switzerland, Australia, England and Ireland.	England, India, Serbia, and the United States

Product(s) and Services	In what countries does CIBT store Customer Personal Data?	In what countries does CIBT process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
CIBT (all entities) support	Germany (primary), United States, Switzerland, Australia, England	England, EU countries, India, Serbia, United States

When personal data originating from Europe is transferred to CIBT, CIBT relies upon the contractual means that (including the possible use of EU and UK SCC's) to provide an appropriate safeguard for the transfer. To review CIBT's Data Processing Addendum please make a request by sending an email to: legal@cibt.com.

Where customer personal data originating from Europe is transferred between CIBT group companies or transferred by CIBT to third-party sub-processors, CIBT enters into contractual agreement with those parties.

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 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.

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 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.

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 CIBT subject to FISA 702 or EO 12333?

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

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

To date, CIBT 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 CIBT 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.

Security and Protection Measures:

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

- **Encryption:** CIBT offers data encryption at rest and in transit,
- **Security and certifications:** Additional information about CIBT's security practices and certifications are available our Data Processing Addendum.

CIBT's **contractual measures** are set out in our Data Processing Addendum. In particular, we are subject to the following requirements:

- **Technical measures:** CIBT 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 agreement we enter into with customers, service providers, and between entities with the CIBT group).

- **Transparency:** CIBT is obligated to notify its customers in the event it is made subject by a government authority to a request for government access to customer personal data. In the event that CIBT is legally prohibited from making such a disclosure, CIBT is contractually obligated to challenge such prohibition and seek a waiver.

- **Actions to challenge access:** CIBT is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

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

- **Policy for government access:** CIBT publishes and follows CIBT Guidelines for Law Enforcement Requests when responding to any government requests for data. To obtain data from CIBT, 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 CIBT service providers, we remain accountable to you for how it is used. We require all service providers to undergo a thorough cross-functional due diligence process carried out 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 CIBT 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 upon request, based on your use.

- **Privacy by design:** CIBT's Privacy Principles outline CIBT's approach to privacy.
- **Employee training:** CIBT provides data protection training to all CIBT staff.

Procedural steps to implement effective supplementary measures:

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

Re-evaluation at appropriate intervals:

CIBT 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.