# Data Transfer Impact Assessment

*Last updated on: March 10th, 2022*

## Overview

This document provides information to help KnowBe4 customers conduct data transfer impact assessments in connection with their use of KnowBe4 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 KnowBe4 in the US, the safeguards KnowBe4 puts in place in connection with transfers of customer personal data from the European Economic Area, United Kingdom or Switzerland ("Europe"), and KnowBe4's ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

## Step 1: Identify your transfer

Where KnowBe4 processes personal data governed by European data protection laws as a data processor (on behalf of our customers), KnowBe4 complies with its obligations under its Data Processing Addendum available at Data Processing Addendum ("DPA"). The KnowBe4 DPA incorporates the SCCs.

A list of all of our data subprocessors can be found here.

We may transfer customer personal data wherever we or our third-party service providers operate for the purpose of providing you the Subscription Services. The

locations will depend on the particular KnowBe4 Subscription Services you use, as outlined in the chart below.

| **Product(s) and Subscription Services** | **In what countries does KnowBe4 store Customer Personal Data?** | **In what countries does KnowBe4 process (e.g., access, transfer, or otherwise handle) Customer Personal Data?** |
|---|---|---|
| KnowBe4 Kevin Mitnick Security Awareness Training (KMSAT) | Customers can choose main storage in data centers in the United States, European Union, or Canada. However, some data will be hosted and/or processed by subprocessors in the countries specified in the subprocessor listing. | United States, Netherlands, Canada, United Kingdom, Germany, Ireland, Australia, India, Brazil, Japan, Singapore, South Africa, Norway, UAE (Dubai) |

| | | |
|---|---|---|
| PhishER | Customer can choose main storage in data centers in the United States, European Union, or Canada. However, some data will be hosted and/or processed by subprocessors in the countries specified in the subprocessor listing. | United States, Canada, Netherlands, United Kingdom, Ireland, Germany, Australia, India, Brazil, Japan, Singapore, South Africa, Norway, UAE (Dubai) |
| KCM GRC Platform | Customer can choose main storage in data centers in the United States, European Union, or Canada. However, some data will be hosted/and or processed by subprocessors in the countries specified in the subprocessor listing. | United States, Canada, Netherlands, United Kingdom, Ireland, Germany, Australia, India, Brazil, Japan, Singapore, South Africa, Norway, UAE (Dubai) |

| | | |
|---|---|---|
| KnowBe4 Subscription Services support | | United States, Netherlands, United Kingdom, Germany, Australia, India, Brazil, Japan, Singapore, South Africa, Norway, UAE (Dubai) |

## Step 2: Identify the transfer tool relied upon

Where personal data originating from Europe is transferred to KnowBe4, KnowBe4 relies upon the European Commission's approved SCCs to provide an appropriate safeguard for the transfer. To review KnowBe4's Data Processing Addendum (which incorporates the SCCs) please visit Data Processing Addendum.

Where customer personal data originating from Europe is transferred between KnowBe4 affiliates or transferred by KnowBe4 to third-party subprocessors, KnowBe4 enters into SCCs with those parties.

## Step 3: Assess the laws and practices of the recipient countries

### U.S. Surveillance Laws & Responses

| | |
|---|---|
| FISA Section 702 (“FISA 702”) | FISA 702 allows the 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") | EO 12333 authorizes intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. It is our view that our customers' information is highly unlikely to be classified as “foreign intelligence” information under FISA 702. The nature of the data processed by KnowBe4 is not typically the type of data the US government seeks to protect its national interests. |

| | |
|---|---|
| Key findings based on the U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after Schrems II whitepaper. | **Key Findings FISA 702**<br><br>1. Government access to company data is “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.”<br><br>2. There is individual redress, including for EU citizens, for violations of FISA section 702.<br><br>**Key Findings EO 12333**<br><br>1. EO 12333 does not on its own “authorize the U.S. government to require any company or person to disclose data.” EO 12333 relies on a statute, such as FISA 702, in order to collect data.<br><br>2. Bulk data collection, the type of data collection at issue in Schrems II, is expressly prohibited under EO 12333. |

| | |
|---|---|
| Is KnowBe4 subject to FISA 702 or EO 12333? | KnowBe4, like most US-based SaaS companies, could technically be subject to FISA 702 where it is deemed to be a Remote Computing Service Provider ("RCSP"). **However, KnowBe4 does not process personal data that is likely to be of interest to US intelligence agencies.**<br><br>Furthermore, KnowBe4 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. KnowBe4 does not provide internet backbone Subscription Services, but instead only carries traffic involving its own customers (for internal training purposes).<br>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).<br><br>EO 12333 contains no authorization to compel private companies (such as KnowBe4) 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 KnowBe4 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 KnowBe4's practical experience dealing with government access requests?**

KnowBe4 publishes an annual transparency report with information about government requests to access data. To date, KnowBe4 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.

## Step 4: Implement Supplementary Measures

KnowBe4 provides the following **technical measures** to secure customer data:

**Data localization:** KnowBe4 allows customers to choose a primary storage location. The locations are in the jurisdictions listed on the KnowBe4 security page.
**Encryption:** KnowBe4 offers data encryption at rest and in transit.
**Seals, marks, or other certifications:** Additional information about KnowBe4's security practices and certifications on KnowBe4's security page located here. Knowbe4 is ISO 27001, 27701, 27017, and 27018 certified.
**Technical measures:** KnowBe4 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 KnowBe4 group).
**Transparency:** We agree to promptly notify you if we: (i) receive a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred; or (ii) if we become aware of any direct access by public authorities to personal data. Such notification shall include all information available to us. If we are prohibited from notifying you by applicable law, then we agree to use our best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. We agree to document our efforts in order to be able to demonstrate them on request. Where permissible, we agree to provide you with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). We agree to preserve the information for the duration of the contract and make it available to the competent supervisory authority on

request. KnowBe4 additionally maintains a Transparency Report that provides information about requests received from government and law enforcement agencies.
**Actions to challenge access:** Under the SCCs, KnowBe4 is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.
**Policy for government access:** To obtain data from KnowBe4, 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:** It is Knowbe4's policy that all service providers undergo a due diligence process which includes multiple KnowBe4 departments including the privacy, security, and legal team.
**Privacy by design:** KnowBe4's has implemented policies in the Software Development Lifecycle ("SDLC") to ensure privacy principles are adhered to.
**Employee training:** KnowBe4 provides security and privacy training to all KnowBe4 staff on an annual basis.
**Contractual Measures:** KnowBe4's contractual obligations are located in its Data Processing Addendum.

## Step 5: Procedural steps necessary to implement effective supplementary measures

Based on the technical and organizational security measures KnowBe4 has taken and the scope of data processed, KnowBe4 considers that processing EU personal data in/to the US do not impinge on our ability to comply with our requirements under the standard contractual clauses and do not believe any further supplementary measures are needed at this time.

## Step 6: Re-evaluate at appropriate intervals

KnowBe4 will review the risks involved in cross border data transfers and the measures it has implemented to mitigate current and future risks periodically.