Data Transfer Impact Assessment

Last updated on: March 11, 2026

Overview

This document provides information to help KnowBe4 ("we," "us," and "our") customers conduct data transfer impact assessments in connection with their use of KnowBe4 Subscription Services,, 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 United States ("US"), the safeguards KnowBe4 puts in place in connection with transfers of customer Personal Data from the European Economic Area, United Kingdom, or Switzerland (collectively, "Europe"), as well as India, Brazil, Singapore, Australia, the United Arab Emirates, and South Africa (collectively, "Affiliate Countries") where KnowBe4 has affiliates, and KnowBe4's ability to comply with its obligations as a "data importer" under the Standard Contractual Clauses ("SCCs") and United Kingdom International Data Transfer Addendum ("UK IDTA").

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.

Where KnowBe4 processes Personal Data governed by the United Kingdom's 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 may incorporate the UK IDTA where applicable and is available here.

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

https://www.knowbe4.com/hubfs/Data-Transfer-Impact-Assessment.pdf?hsLang=en

We may transfer customer Personal Data wherever we or our third party 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.

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 Security Awareness Training (KSAT) and Security Coach	Customers may choose main storage in data centers in the United States, Ireland, Germany, the United Kingdom, 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, UAE (Dubai)
PhishER	Customer may choose main storage in data centers in the United States, Ireland, Germany, the United Kingdom, 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, UAE (Dubai)

KCM GRC Platform	Customer may choose main storage in data centers in the United States or Europe. 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, UAE (Dubai)
KnowBe4 Subscription Services support		United States, Netherlands, United Kingdom, Germany, Australia, India, Brazil, Japan, Singapore, South Africa, UAE (Dubai)
HRM+ and Cloud Email Security (This includes Defend, Prevent, Protect)	Customer may choose main storage in data centers in the United States, Ireland, Germany, the United Kingdom, or Canada. However, some data will be hosted and/or processed by subprocessors in the countries specified in the subprocessor listing.	United States, Netherlands, United Kingdom, Germany, Australia, India, Brazil, Japan, Singapore, South Africa, 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.

Where customer Personal Data originating from the United Kingdom is transferred between KnowBe4 affiliates or transferred by KnowBe4 to third party subprocessors, KnowBe4 enters into the UK IDTA with those parties.

https://www.knowbe4.com/hubfs/Data-Transfer-Impact-Assessment.pdf?hsLang=en

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

United States

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 US Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-US Data Transfers after Schrems II whitepaper.	**Key Findings FISA 702** 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 U.S. intelligence agencies would seek to collect that data." 2. There is individual redress, including for EU citizens, for violations of FISA section 702. **Key Findings EO 12333** 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. 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.** 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). To date, the US 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 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.

India

Section	Description
Purpose for Transfer and Any Further Processing	For the purposes of assisting in the provision of Services.

Frequency of the Transfer	Onward transfers to India are continuous, supporting ongoing service provision and development.
Categories of Personal Data Transferred	As specified on the sub-processor listing.
Sensitive Data Transferred (if applicable)	The transfer of sensitive data is determined at the sole discretion of the data exporter, with appropriate safeguards in place to protect such data in accordance with legal requirements.
Applicable Transfer Mechanism	Standard Contractual Clauses and further security measures outlined in the appendix, ensuring that appropriate technical and organizational measures as required by data protection law.
Identifying Laws and Practices Relevant considering the circumstances of the transfer	India's surveillance, criminal, and security laws allow government agencies to intercept and access personal information and sensitive personal data without obtaining prior consent under certain conditions. Key laws include: Information Technology Act, 2000; Indian Telegraph Act, 1885; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; Criminal Laws and Code of Criminal Procedure, 1973.
Assessment of the Law and Practices in India	Given the scope of India's surveillance and interception powers, data recipients in India are potentially within the scope of such laws for criminal law enforcement and may be obligated to share data with government authorities. KnowBe4 adheres to its security measures located in the appendix and publishes an annual Transparency Report on government data requests.

https://www.knowbe4.com/hubfs/Data-Transfer-Impact-Assessment.pdf?hsLang=en

Brazil

Section	Description
Purpose for Transfer and Any Further Processing	For the purposes of assisting in the provision of Services.
Frequency of the Transfer	Continuous.
Categories of Personal Data Transferred	As specified on the sub-processor listing.
Sensitive Data Transferred (if applicable)	Determined at the sole discretion of the data exporter.
Applicable Transfer Mechanism	Standard Contractual Clauses and further security measures outlined in the appendix, ensuring that appropriate technical and organizational measures as required by data protection law.
Identifying Laws and Practices Relevant considering the circumstances of the transfer	The Brazilian government can only access/intercept personal data for specified purposes, such as criminal law enforcement and surveillance, after court authorization. Key laws include the Wiretapping and Information Systems Surveillance Law, Brazilian Intelligence Agency (ABIN) regulations, the Brazilian Internet Civil Rights Framework, and the Brazilian General Data Protection Law (LGPD), which is aligned with the GDPR.

Assessment of the Law and Practices in Brazil	The Brazilian government can access/intercept personal data for specified purposes, such as criminal law enforcement and surveillance, only after court authorization. Relevant laws include the Wiretapping and Information Systems Surveillance Law, Brazilian Intelligence Agency regulations, the Brazilian Internet Civil Rights Framework, and the Brazilian General Data Protection Law (LGPD), which is aligned with the GDPR but does not cover national security or criminal matters. KnowBe4 adheres to its security measures located in the appendix and publishes an annual Transparency Report on government data requests.

Singapore

Section	Description
Purpose for Transfer and Any Further Processing	For the purposes of assisting in the provision of Services.
Frequency of the Transfer	Continuous.
Categories of Personal Data Transferred	As specified on the sub-processor listing.
Sensitive Data Transferred (if applicable)	Determined at the sole discretion of the data exporter.
Applicable Transfer Mechanism	Standard Contractual Clauses and further security measures outlined in the appendix, ensuring that appropriate technical and organizational measures as required by data protection law.

Identifying Laws and Practices Relevant considering the circumstances of the transfer	Singapore has enacted laws that enable the government to obtain access to data including personal data being processed in Singapore. Key laws include: The Cybersecurity Act, The Protection from Harassment Act, The Computer Misuse Act, and The Personal Data Protection Act (PDPA).
Assessment of the Law and Practices	Although not explicitly detailed in the provided text, based on the laws mentioned, Singapore's legal framework provides for both the protection of personal data and mechanisms for government access under certain conditions. KnowBe4 adheres to its security measures located in the appendix and publishes an annual Transparency Report on government data requests.

Australia

Section	Description
Purpose for Transfer and Any Further Processing	For the purposes of assisting in the provision of Services.
Frequency of the Transfer	Continuous.
Categories of Personal Data Transferred	As specified on the sub-processor listing.

Sensitive Data Transferred (if applicable)	Determined at the discretion of the data exporter.
Applicable Transfer Mechanism	Standard Contractual Clauses and further security measures outlined in the appendix, ensuring that appropriate technical and organizational measures as required by data protection law.
Identifying Laws and Practices Relevant considering the circumstances of the transfer	Australia's laws, such as the Crimes Act 1914, Surveillance Devices Act 2004, and Telecommunications (Interception and Access) Act 1979, grant authorities the power to access data under certain conditions.
Assessment of the Law and Practices	The legislative framework in Australia grants government authorities the power to access electronic and physical data, with certain laws having potential extraterritorial reach. However, such access is generally bound by bilateral processes like mutual legal assistance treaties. KnowBe4 adheres to its security measures located in the appendix and publishes an annual Transparency Report on government data requests.

United Arab Emirates (UAE)

Section	Description
Purpose for Transfer and Any Further Processing	For the purpose of providing customer support (where applicable).

Frequency of the Transfer	Continuous
Categories of Personal Data Transferred	As specified on the sub-processor listing.
Sensitive Data Transferred (if applicable)	Determined at the discretion of the data exporter.
Applicable Transfer Mechanism	Standard Contractual Clauses and further security measures outlined in the appendix, ensuring that appropriate technical and organizational measures as required by data protection law.
Identifying Laws and Practices Relevant considering the circumstances of the transfer	Relevant UAE laws may include the DIFC Data Protection Law, ADGM Data Protection Regulations, Cyber Crimes Law, and TRA Guidelines.
Assessment of the Law and Practices in the UAE	The UAE's evolving data protection landscape requires careful monitoring to ensure compliance with local laws, which include measures for privacy protection and data security, as well as provisions for government access to data under certain conditions. KnowBe4 adheres to its security measures located in the appendix and publishes an annual Transparency Report on government data requests.

https://www.knowbe4.com/hubfs/Data-Transfer-Impact-Assessment.pdf?hsLang=en

South Africa

Section	Description
Purpose for Transfer and Any Further Processing	For the purposes of assisting in the provision of Services.
Frequency of the Transfer	Continuous.
Categories of Personal Data Transferred	As specified on the sub-processor listing.
Sensitive Data Transferred (if applicable)	Determined at the sole discretion of the data exporter.
Applicable Transfer Mechanism	Standard Contractual Clauses and further security measures outlined in the appendix, ensuring that appropriate technical and organizational measures as required by data protection law.
Identifying Laws and Practices Relevant considering the circumstances of the transfer	South Africa's legal framework for personal data protection includes the Protection of Personal Information Act (POPIA) and the Electronic Communications and Transactions Act, 2002 (ECTA). POPIA regulates the processing of personal data and includes provisions for data subject rights, data breach notifications, and the appointment of an Information Regulator. ECTA includes provisions related to electronic transactions and the protection of personal information collected electronically.

Assessment of the Law and Practices	South Africa's legal framework aims to protect personal data by setting strict processing conditions and providing mechanisms for accountability and enforcement through POPIA and ECTA. KnowBe4 adheres to its security measures located in the appendix and commits to transparency in its dealings with government data requests.

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 our security practices and certifications are listed on the KnowBe4 Security page. 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 (under both (i) the Data Processing Addendum and (ii) the SCCs we enter into with customers, service providers, and between entities within 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 upon request. Where permissible, we agree to provide you with as much relevant information as possible on the requests received (in particular, the 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 Agreement and to 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, a court order, or a warrant.
- **Onward transfers:** It is KnowBe4 policy that all service providers undergo a due diligence process that includes review by multiple departments, including the KnowBe4 privacy, security, and legal teams.
- **Privacy by design:** KnowBe4 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 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 processing EU Personal Data in/to the US or does not impinge on our ability to comply with our requirements under the SCCs, or UK ITDA, or Affiliate Countries and does 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 we have implemented to mitigate current and future risks periodically.