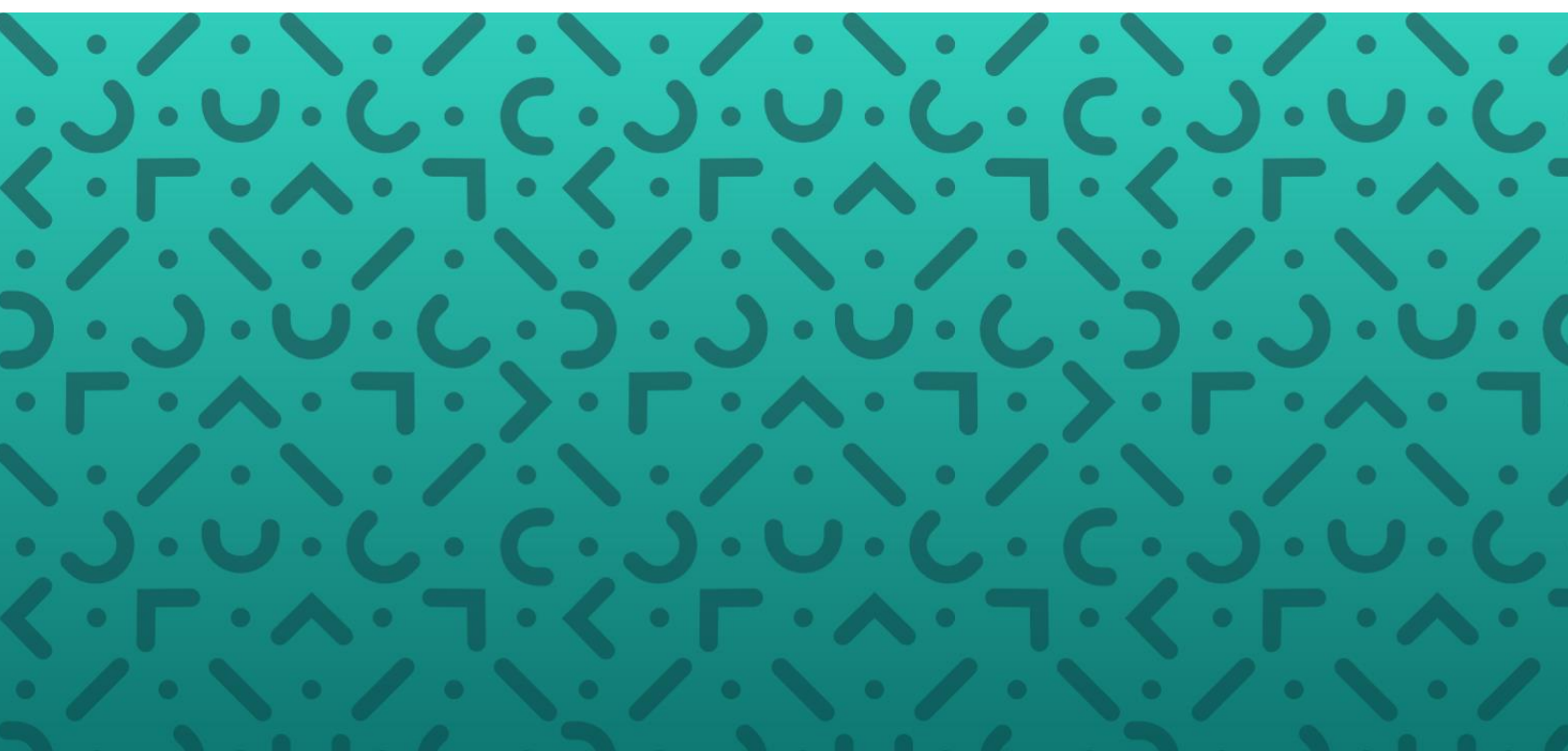




Transfer Risk and Impact Statement

May 19, 2022



Overview

The privacy landscape is dynamic. UKG has adopted privacy principles from the European Union's General Data Protection Regulation ("GDPR") as the foundation for our privacy program. These principles provide a consistent baseline for privacy in the development and operations of UKG's products and services and allow us to adapt to changes in the privacy landscape as they occur.

In response to Schrems II and Recommendations 2020/1 and 2020/2, UKG relies on Module 2 and Module 3 of the [standard contractual clauses](#) (SCCs) adopted on June 4, 2021, and the UK International Data Transfer Agreement adopted on March 21st, 2022 (UK IDTA) as the mechanism that enables cross-border transfers of personal data between the EEA/UK and jurisdictions that are neither European Economic Area (EEA) members nor deemed adequate by the EU in accordance with Article 5 of the GDPR. UKG has incorporated those SCCs and the UK IDTA into its [Data Protection Addendum](#) (DPA).

When we process our customers' personal data, UKG is a data processor. UKG might use other processors (i.e., subprocessors) in order to provide the personal data processing requested by our customer as is more specifically set forth in our customer agreements. UKG also has agreements in place with its subprocessors, which include written assurances designed to ensure the consistent and appropriate processing and safeguarding of personal data. A customer can find additional information about our use of subprocessors in our [list of subprocessors](#). Please refer to the appropriate links below for product-specific information about our personal data handling and safeguards.

UKG believes that a customer should control the information that they collect, create, communicate, and store about their workforce. UKG does not give anyone access to a customer's information unless the customer instructs us to do so, provides consent, or we are legally obligated to do so. UKG does not support "back door" direct access to its operations (including our data stores) by any government. UKG does not share its encryption keys or provide the ability to break its encryption keys to any government.

As a processor, UKG encrypts personal data when it is stored and while it is transmitted. UKG limits access to and encrypts its encryption keys. UKG does not support a "bring your own keys" option for its customers as data is stored at the database level, and not on the file level. UKG maintains its privacy and security programs in a manner that complies with its customer agreements. This includes our [DPA](#) and security addendum, which describe our programs and practices with respect to privacy and data security. Depending on the product purchased and applications in use by the customer, UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports. Please refer to the appropriate links below for product specific-security certifications.

Outcome Statement

Based on the information in this Statement, UKG has determined that it can proceed with the transfer of EEA/UK personal data to countries outside of the EEA (commonly referred to as third countries). UKG's transfers of EEA/UK personal data to third countries are subject to the SCCs and the UK IDTA, which impose obligations intended to ensure EEA/UK personal data transferred to third countries is afforded a level of protection that is essentially equivalent to that guaranteed by the data protection laws of the EEA and/or the United Kingdom. Furthermore, UKG has no reason to believe that any laws that exist in the third countries to which it transfers personal data will be interpreted and/or applied in practice to cover UKG's transfer of EEA personal data to these third countries.

Table of Contents

- Overview.....1

- Outcome Statement.....2

- Product-Specific Information4
 - UKG Dimensions4
 - UKG Pro6
 - UKG Ready8
 - UKG Workforce Central10
 - UKG HR Service Delivery.....12

- Country-Specific Information14
 - USA14
 - AUSTRALIA.....17
 - INDIA.....19
 - SINGAPORE20

Please reach out to Privacy@UKG.com for information about transfers of EEA/UK personal data to countries outside of the EEA/UK with respect to products not listed in this Transfer Risk and Impact Statement.



Product-Specific Information

UKG Dimensions

UKG Dimensions			
Where is the importer located?	USA	INDIA	AUSTRALIA
Will the importer be forwarding the data to another organization?	Yes	No	No
If yes, what kind of organization is it, and where is it located?	UKG Subprocessors & Affiliates	N/A	N/A
Why are you making the transfer?	Cross-border transfer is necessary for customer onboarding and customer support.	Cross-border transfer is necessary for customer support.	Cross-border transfer is necessary for customer support.
What will the importer (and any other party to whom it forwards the data) be doing with the personal data?	Recipient will engage in personal data processing (storage, access, manipulation, and retention) to complete customer onboarding and provide customer support.	Recipient will engage in personal data processing (access, manipulation, and retention) to provide customer support.	Recipient will engage in personal data processing (access, manipulation, and retention) to provide customer support.
What security certifications does UKG maintain?	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.
Who is the data about?	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.

What type(s) of data are you transferring?	The product processes personal data related to human capital management and other data as determined by the customer.	The product processes personal data related to human capital management and other data as determined by the customer.	The product processes personal data related to human capital management and other data as determined by the customer.
How is the data sent?	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.
For how long can the importer (and other recipients) access the data?	Access to personal data is role-based with privileges assigned on a need-to-know basis. Personal data retention is established by the customer. Access to customer data is only needed until the customer's implementation is complete or the customer's support request is complete.	Access to personal data is role-based with privileges assigned on a need-to-know basis. Access is view only. Personal data may be accessed from but is not saved or retained in India. Access to customer data is only needed until the customer's support request is complete.	Access to personal data is role-based with privileges assigned on a need-to-know basis. Access is view only. Personal data may be accessed from but is not saved or retained in Australia. Access to customer data is only needed until the customer's support request is complete.
How often will these transfers occur?	Cross-border transfers for the purposes of onboarding occur during the implementation phase of the service. Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer's needs.	Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer's needs.	Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer's needs.

UKG Pro

UKG Pro			
Where is the importer located?	USA	SINGAPORE	INDIA
Will the importer be forwarding the data to another organization?	Yes	No	No
If yes, what kind of organization is it, and where is it located?	UKG Subprocessors & Affiliates	N/A	N/A
Why are you making the transfer?	Cross-border transfer is necessary for customer onboarding and customer support.	Cross-border transfer is necessary for customer support.	Cross-border transfer is necessary for customer onboarding.
What will the importer (and any other party to whom it forwards the data) be doing with the personal data?	Recipient will engage in personal data processing (storage, access, manipulation, and retention) to complete customer onboarding and provide customer support.	Recipient will engage in personal data processing (access, manipulation, and retention) to provide customer support.	Recipient will engage in personal data processing (access, manipulation, and retention) to complete customer onboarding.
What security certifications does UKG maintain?	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.
Who is the data about?	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.
What type(s) of data are you transferring?	The product processes personal data related to human capital	Data transferred is only for security analysis purposes: log data,	The product processes personal data related to human capital

	management and other data as determined by the customer. Data transferred is also for security analysis purposes: log data, credentials, IP addresses, employee IDs, company name, account numbers, bank names, routing numbers.	credentials, IP addresses, employee IDs, company name, account numbers, bank names, routing numbers.	management and other data as determined by the customer.
How is the data sent?	Data may be remote accessed via VPN, SSL, and AES-256 bit encryption. Data may also be sent encrypted via SFTP, PGP, SSL, or TLS.	Data may be remote accessed via VPN, SSL, and AES-256 bit encryption. Data may also be sent encrypted via SFTP, PGP, SSL, or TLS.	Data may be remote accessed via VPN, SSL, and AES-256 bit encryption. Data may also be sent encrypted via SFTP, PGP, SSL, or TLS.
For how long can the importer (and other recipients) access the data?	UKG and its subprocessors only engage in personal data processing as instructed and as described in its agreement with its customer, to comply with applicable laws, or for other legitimate interests.	UKG and its subprocessors only engage in personal data processing as instructed and as described in its agreement with its customer, to comply with applicable laws, or for other legitimate interests.	UKG and its subprocessors only engage in personal data processing as instructed and as described in its agreement with its customer, to comply with applicable laws, or for other legitimate interests.
How often will these transfers occur?	Transfers will occur per the agreed-upon delivery of services detailed within the contractual commitment UKG has with the customer or upon customer instruction.	Transfers will occur per the agreed-upon delivery of services detailed within the contractual commitment UKG has with the customer or upon customer instruction.	Transfers will occur per the agreed-upon delivery of services detailed within the contractual commitment UKG has with the customer or upon customer instruction.

UKG Ready

UKG Ready			
Where is the importer located?	USA	INDIA	AUSTRALIA
Will the importer be forwarding the data to another organization?	Yes	No	No
If yes, what kind of organization is it, and where is it located?	UKG Subprocessors & Affiliates	N/A	N/A
Why are you making the transfer?	Cross-border transfer is necessary for customer onboarding and customer support.	Cross-border transfer is necessary for customer support.	Cross-border transfer is necessary for customer support.
What will the importer (and any other party to whom it forwards the data) be doing with the personal data?	Recipient will engage in personal data processing (storage, access, manipulation, and retention) to complete customer onboarding and provide troubleshooting assistance to the customer.	Recipient will engage in personal data processing (access, manipulation, and retention) to provide troubleshooting assistance to the customer.	Recipient will engage in personal data processing (access, manipulation, and retention) to provide troubleshooting assistance to the customer.
What security certifications does UKG maintain?	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.
Who is the data about?	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.

What type(s) of data are you transferring?	The product processes personal data related to human capital management and other data as determined by the customer.	The product processes personal data related to human capital management and other data as determined by the customer.	The product processes personal data related to human capital management and other data as determined by the customer.
How is the data sent?	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.
How long can the importer (and other recipients) access the data?	Support and Professional Services personnel have “SA” (system admin) access to the customer’s account on an as-needed basis. These admin-level accounts have read only access. Access is only given to support staff based on need. This is for the EU support staff first and foremost, and then additional users are added from the U.S. support teams to only those who need access for either additional/overflow support resources or second- or third-tier support (i.e., Solutions/Shared Services).	Support and Professional Services personnel have “SA” (system admin) access to the customer’s account. These admin-level accounts have read only access. Access is only given to support staff based on need. This is for the EU support staff first and foremost, and then additional users are added from the U.S., Indian and Australian support teams to only those who need access for either additional/overflow support resources or second- or third-tier support (i.e., Solutions/Shared Services).	Support and Professional Services personnel have “SA” (system admin) access to the customer’s account. These admin-level accounts have read only access. Access is only given to support staff based on need. This is for the EU support staff first and foremost, and then additional users are added from the U.S., Indian and Australian support teams to only those who need access for either additional/overflow support resources or second- or third-tier support (i.e., Solutions/Shared Services).
How often will these transfers occur?	Cross-border transfers for the purposes of onboarding occur during the implementation phase of the service. Cross-border transfers for the purposes of support occur on an episodic	Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer’s needs.	Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer’s needs.

	basis as determined by the customer's needs.		
--	--	--	--

UKG Workforce Central

UKG Workforce Central			
Where is the importer located?	USA	INDIA	AUSTRALIA
Will the importer be forwarding the data to another organization?	Yes	No	No
What kind of organization is it, and where is it located?	UKG Subprocessors & Affiliates	N/A	N/A
Why are you making the transfer?	Cross-border transfer is necessary for customer onboarding and customer support.	Cross-border transfer is necessary for customer support.	Cross-border transfer is necessary for customer support.
What will the importer (and any other party to whom it forwards the data) be doing with the personal data?	Recipient will engage in personal data processing (storage, access, manipulation, and retention) to complete customer onboarding and provide troubleshooting assistance to the customer.	Recipient will engage in personal data processing (access, manipulation, and retention) to provide trouble shooting assistance to customer.	Recipient will engage in personal data processing (access, manipulation, and retention) to provide trouble shooting assistance to customer.
What security certifications does UKG maintain?	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.

Who is the data about?	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.	Personal data might concern employees and former employees of the customer.
What type(s) of data are you transferring?	The product processes personal data related to human capital management and other data as determined by the customer.	The product processes personal data related to human capital management and other data as determined by the customer.	The product processes personal data related to human capital management and other data as determined by the customer.
How is the data sent?	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.
For how long can the importer (and other recipients) access the data?	Support and Professional Services personnel access customer's system via a set of support accounts – ADM and Ops. ADM has full admin privileges, and Ops has basic admin privileges (read and write only). Both accounts – when enabled – have access to all employee data except in the case of extensions for healthcare customers. This data is not visible to UKG employees and requires access to the customer's encryption gateway to see any customer data. Access to the customer's data is only needed until the customer's implementation is complete or the support request is complete and the data is no longer required	Support and Professional Services personnel access customer's system via a set of support accounts – ADM and Ops. ADM has full admin privileges, and Ops has basic admin privileges (read and write only). Both accounts – when enabled – have access to all employee data except in the case of extensions for healthcare customers. This data is not visible to UKG employees and requires access to the customer's encryption gateway to see any customer data. Access to the customer's data is only needed until the customer support request is complete and the data is no longer required per internal procedures.	Support and Professional Services personnel access customer's system via a set of support accounts – ADM and Ops. ADM has full admin privileges, and Ops has basic admin privileges (read and write only). Both accounts – when enabled – have access to all employee data except in the case of extensions for healthcare customers. This data is not visible to UKG employees and requires access to the customer's encryption gateway to see any customer data. Access to the customer's data is only needed until the customer support request is complete and the data is no longer required per internal procedures.

	per internal procedures.		
How often will these transfers occur?	Cross-border transfers for the purposes of onboarding occur during the implementation phase of the service. Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer's needs.	Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer's needs.	Cross-border transfers for the purposes of support occur on an episodic basis as determined by the customer's needs.

UKG HR Service Delivery

UKG HR Service Delivery			
Where is the importer located?	USA	INDIA	SINGAPORE
Will the importer be forwarding the data to another organization?	Yes	No	No
If yes, what kind of organization is it, and where is it located?	UKG Subprocessors & Affiliates	N/A	N/A
Why are you making the transfer?	Cross-border transfer is necessary for customer support.	Cross-border transfer is necessary for customer support and cloud security monitoring.	Cross-border transfer is necessary for customer support and cloud security monitoring.
What will the importer (and any other party to whom it forwards the	Recipient will engage in personal data processing (storage, access, manipulation, and retention) to	Recipient will engage in personal data processing (access, manipulation, and retention) to provide	Recipient will engage in personal data processing (access, manipulation, and retention) to provide

data) be doing with the personal data?	provide troubleshooting assistance to the customer.	troubleshooting assistance to the customer.	troubleshooting assistance to the customer.
What security certifications does UKG maintain?	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.	UKG maintains ISO 27001, ISO 27017, and ISO 27018 certifications and SOC 1 and SOC 2 reports.
Who is the data about?	Employees, agents, contractors, advisers, professional experts, and contacts.	Employees, agents, contractors, advisers, professional experts, and contacts.	Employees, agents, contractors, advisers, professional experts, and contacts.
What type(s) of data are you transferring?	The product processes personal data related to human capital management data and disclosed in the database. There is no access to the data subjects' documents (HR Core Data).	The product processes personal data related to human capital management data and disclosed in the database. There is no access to the data subjects' documents (HR Core Data).	The product processes personal data related to human capital management data and disclosed in the database. There is no access to the data subjects' documents (HR Core Data).
How is the data sent?	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.	Data is sent encrypted via SFTP or TLS.
For how long can the importer (and other recipients) access the data?	UKG and its subprocessors only engage in personal data processing as instructed and as described in its agreement with its customer, to comply with applicable laws, or for other legitimate interests.	Support and Professional Services personnel have "SA" (system admin) access to the customer's account. These admin-level accounts have read-only access. Access is only given based on need.	Support and Professional Services personnel have "SA" (system admin) access to the customer's account. These admin-level accounts have read-only access. Access is only given based on need.
How often will these transfers occur?	Transfers will occur per the agreed-upon delivery of services	Cross-border transfers for the purposes of support occur on an	Cross-border transfers for the purposes of support occur on an

	detailed within the contractual commitment UKG has with the customer or upon customer instruction.	episodic basis as determined by the customer's needs.	episodic basis as determined by the customer's needs.
--	--	---	---

Country-Specific Information

USA

USA	
Are the contractual safeguards likely to be enforceable in the destination country?	Yes. The U.S. recognizes the rule of law, as there is an established and respected legal and court system. Foreign judgments or arbitration awards can be enforced. Under U.S. law, an individual seeking to enforce a foreign judgment, decree, or order in the U.S. must file suit before a competent court. The court will determine whether to recognize and enforce the foreign judgment. The U.S. has been a member of the Hague Conference on Private International Law since October 15, 1964, and is now a contracting state to six conventions of the Hague Conference, including the Choice of Court Convention. There is ready access to justice through the court system, which provides means for redress and effective remedies. The rights of third-party beneficiaries under contracts are recognized and enforced. There are high levels of integrity and independence in the judicial process. The UK is currently evaluating the possibility of finding adequacy for the U.S. with respect to privacy regulations.
Are there laws that set out when and how the law can require access to data be given to third parties, including public authorities?	Yes. Public authorities or third parties cannot access data from private companies, including to intercept communications, without meaningful safeguards (for example, court order or warrant). Organizations can undertake workplace monitoring, but there are significant safeguards.
Are there limitations on how third parties, including public	Yes. Public and private authorities may only use the data they access or receive from third parties for justified and limited purposes – for

authorities, can use the data they access?	example, in the case of public authorities, for law enforcement, protection of public health, and safeguarding national security.
Do individuals have effective and enforceable rights and remedies in relation to the safeguards for third-party access?	Yes. There are clear and enforceable rights in place to allow individuals access to their personal data, and individuals may readily seek judicial challenge of private and public authorities accessing their data, including by using surveillance measures.
Is there effective oversight?	Yes. Police and intelligence agencies operate with clear judicial or other effective administrative oversight of their activities.
Does the destination country have mature data protection and/or privacy laws in place?	In the U.S. the Constitution does not expressly address individual privacy. The U.S. Supreme Court has inferred a right to privacy in its decisions citing to language in the First, Third, Fourth, Fifth, and Ninth amendments. Instead of omnibus federal privacy legislation, the U.S. has a patchwork of sector-specific privacy legislation and regulations that restrict the processing of personal data. These laws address information concerning an individual's taxes (IRS rules), consumer credit (FCRA), financial accounts (GLBA), education records (FERPA), health information (HIPAA), and the like. The U.S. Federal Trade Commission (FTC) has performed privacy and security enforcement for nearly 50 years, for the FCRA and more recently for the Safe Harbor and Privacy Shield programs. The FTC also takes action for unfair or deceptive trade practices against entities when personal data processing is inconsistent with its privacy notice. Additionally, each of the U.S. states and protectorates has authority to enact its own legislation and regulations for privacy and data protection. While many state laws focus on protection for consumers, the effect of these laws can be quite broad, such as the application of California's CCPA and CPRA legislation to personal data collected in the employment context. The patchwork of federal and state laws, when combined with inferred constitutional protections, provides a framework for the protection of personal data.
Is there a legal framework governing the use of biometrics or facial recognition?	In the U.S., biometric and facial recognition are not addressed at the national level. Not all states have laws addressing these matters, and among those that do, there are inconsistencies.
What other factors should be considered?	There is a history of respect for human rights (in particular, the rights to privacy, freedom of expression, and access to justice). FISA Section 702 cannot be used to investigate ordinary crimes. Instead, the surveillance under FISA Section 702 is largely restricted to specific areas of national defense, national security, and the

conduct of foreign affairs, with an emphasis on international terrorism, sabotage, the proliferation of weapons of mass destruction, and other grave hostile acts.

As a result, FISA Section 702 is limited in scope. First, “foreign intelligence information” must have some nexus to a “foreign power or foreign territory.” This means that most private business or customer records likely will not constitute “foreign intelligence information.” Second, in examining what organizations may be affected by FISA Section 702, the term “foreign power” as defined by the statute primarily incorporates foreign terrorist organizations, foreign governments, and instrumentalities of both. This means that most private businesses likely will not be considered a “foreign power.”

Executive Order 12333 likely has limited to no relevance to transfers of EEA Personal Data to the United States as it generally applies to surveillance activities that are conducted wholly outside of the United States.

Additionally, UKG has assessed that it is not an “electronic communications service provider” under FISA 702 or Executive Order 12333 and therefore is not subject to access requests.

The Cloud Act allows US government access to data in criminal investigations and where there is a threat to the public order, subject to a warrant. UKG does not voluntarily hand over personal information from its customers.

Apart from this, UKG has not built in any backdoors that would allow government authorities to circumvent its security measures to access service data. All of this should therefore mean that UKG has implemented additional measures that adequately address any risk of essential equivalence created by third country regulations.

AUSTRALIA

AUSTRALIA	
Are the contractual safeguards likely to be enforceable in the destination country?	Yes. Australia recognizes the rule of law, as there is an established and respected legal and court system. Foreign judgments or arbitration awards can be enforced. Enforcement of foreign judgments in Australia is governed by both statutory regimes and common law principles. With respect to statutory regimes, the Foreign Judgments Act 1991 and the Foreign Judgments Regulations 1992 provide for the procedure and scope of the judgments that can be enforceable under the statutory regime. Additionally, Australia is party with the United Kingdom to the bilateral treaty for the Reciprocal Recognition and Enforcement of Judgments in Civil and Commercial Matters 1994. However, Australia is not party to the Hague Convention on Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters 1971. In instances when there is no international or statutory agreement, the foreign judgment must be enforced under common law principles.
Are there laws that set out when and how the law can require access to data be given to third parties, including public authorities?	Yes. Public authorities or third parties cannot access data from private companies, including by intercepting communications, without meaningful safeguards – for example, a court order or a warrant. Organizations can undertake workplace monitoring, but there are significant safeguards.
Are there limitations on how third parties including public authorities can use the data it accesses?	Yes. Public and private authorities may only use the data it accesses or receives from third parties for justified and limited purposes. E.g. in the case of public authorities, for law enforcement, protection of public health and safeguarding national security.
Do individuals have effective and enforceable rights and remedies in relation to the safeguards for third-party access?	Yes. There are clear and enforceable rights in place to allow individuals access to their personal data, and individuals may readily seek judicial challenge of private and public authorities accessing their data, including by using surveillance measures.
Is there effective oversight?	Yes. Police and intelligence agencies operate with clear judicial or other effective administrative oversight of their activities.
Does the destination country have mature data protection and/or privacy laws in place?	Data privacy and protection are regulated in Australia by a combination of federal, state, and territory laws. The Privacy Act 1988 (Cth), which includes the Australian Privacy Principles (APPs), is the core privacy legislation in Australia. The Privacy Act applies to private-

	<p>sector entities (with an annual turnover of >AU\$3 million) and all commonwealth government agencies, as well as other specific businesses not meeting the turnover thresholds, including private health service providers processing health information, credit-reporting bodies, and businesses that sell or purchase personal data (APP entities). Most states and territories also have their own (broadly aligned) privacy legislation that is applicable to state government agencies and private businesses that contract with them. In addition to the Privacy Act, APPs, and state privacy laws, there is also specific sector-focused legislation that regulates privacy and information risk – for example, in the health sector and in the telecommunications sector. There is also other legislation at the commonwealth and state levels that is relevant to privacy and the use of personal data, including the Spam Act 2003 (Cth), the Do Not Call Register Act 2006 (Cth), criminal laws prohibiting unauthorized access to computer systems, and various surveillance and listening-devices legislation. More recently, the Treasury Laws Amendment (Consumer Data Right) Act 2019 introduces a consumer-directed data portability mechanism, applicable currently to the banking sector. Further, specific regulators have issued (non-statutory/non-mandatory) standards that instruct regulated entities with regard to specified data protection measures that should be put in place. For example, the Australian Prudential and Regulatory Authority (APRA) regulates financial services institutions and has introduced a number of “prudential” standards on privacy and information risk. Finally, the Australian Consumer Law (ACL) prohibits applicable businesses (including digital platforms) carrying on business in Australia from engaging in certain forms of conduct in connection with the supply or acquisition of goods or services. This includes misleading or deceptive conduct, unconscionable conduct, and unfair practices. Each of these prohibitions under the ACL have been recently cited by the Australian Competition and Consumer Commission (ACCC) (as regulator) as applicable to the privacy practices of an organization, including representations and statements made as to how users’ data is collected and disclosed, including under privacy policies and terms of use.</p>
<p>Is there a legal framework governing the use of biometrics or facial recognition?</p>	<p>In Australia, the Privacy Act 1988 (Cth) governs the way personal data, including biometric data, is collected and used.</p>
<p>What other factors should be considered?</p>	<p>There is a history of respect for human rights (in particular, the rights to privacy, freedom of expression, and access to justice).</p>

INDIA

INDIA	
Are the contractual safeguards likely to be enforceable in the destination country?	Yes. India recognizes the rule of law, as there is an established and respected legal and court system. In India, judgments from courts in “reciprocating territories” can be enforced directly by filing before an Indian court, and execution decree. India is a member of the Hague Conference. There is ready access to justice through the court system, which provides means for redress and effective remedies. The rights of third-party beneficiaries under contracts are recognized and enforced. There are high levels of integrity and independence in the judicial process. The UK is currently evaluating the possibility of finding adequacy for India with respect to privacy regulations.
Are there laws that set out when and how the law can require access to data be given to third parties, including public authorities?	Yes. Public authorities or third parties cannot access data from private companies, including by intercepting communications, without meaningful safeguards (for instance, a court order or a warrant). Organizations can undertake workplace monitoring, but there are significant safeguards.
Are there limitations on how third parties, including public authorities, can use the data they access?	Yes. Public and private authorities may only use the data they access or receive from third parties for justified and limited purposes – for example, in the case of public authorities, for law enforcement, protection of public health, and safeguarding national security.
Do individuals have effective and enforceable rights and remedies in relation to the safeguards for third-party access?	Yes. There are clear and enforceable rights in place to allow individuals access to their personal data, and individuals may readily seek judicial challenge of private and public authorities accessing their data, including, surveillance measures.
Is there effective oversight?	Yes. Police and intelligence agencies operate with clear judicial or other effective administrative oversight of their activities.
Does the destination country have mature data protection and/or privacy laws in place?	In India, privacy protections are rooted in interpretation of its constitution (Article 21 implies privacy as a fundamental right) as well as sector-specific data protection legislation and regulation. Sectoral laws address personal data handling and personal data protection focusing on confidentiality limitation of personal data use. The omnibus legislation, the Personal Data Protection (PDP) Bill, was introduced in 2019. If enacted, PDP will repeal 43A of the Information Technology Act 2000 (IT Act), which addresses the handling of

	personal data and sensitive personal data, affording individual rights similar to those of the GDPR.
Is there a legal framework governing the use of biometrics or facial recognition?	The collection, storage, and handling of biometric data are governed by the Information technology law contained under the IT Act, primarily through the rules framed under it. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) lay out the specific conditions that regulate personal data and sensitive personal data or information, including biometric data.
What other factors should be considered?	There is a history of respect for human rights (in particular, the rights to privacy, freedom of expression, and access to justice).

SINGAPORE

SINGAPORE	
Are the contractual safeguards likely to be enforceable in the destination country?	<p>Yes. Singapore recognizes the rule of law, as there is an established and respected legal and court system. Foreign judgments or arbitration awards can be enforced. Under Singapore law, an individual seeking to enforce a foreign judgment, decree, or order in Singapore must file suit before a competent court. The court will determine whether to recognize and enforce the foreign judgment. Singapore has been a member of the Hague Conference on Private International Law since April 9, 2014, and is now a contracting state to four conventions of the Hague Conference, including the Choice of Court Convention. Singapore is also a contracting state to the New York Arbitration Convention on the Recognition and Enforcement of Foreign Arbitral Awards.</p> <p>There is ready access to justice through the court system, which provides means for redress and effective remedies. The rights of third-party beneficiaries under contracts are recognized and enforced. There are high levels of integrity and independence in the judicial process. The UK is currently evaluating the possibility of finding adequacy for Singapore with respect to privacy regulations.</p>
Are there laws that set out when and how the law can require access to data be	Under the Personal Data Protection Act (PDPA) of 2012, private-sector data controllers and processors have direct obligations to comply with consent obligations for the purposes of collection, use,

<p>given to third parties, including public authorities?</p>	<p>or disclosing of personal data for purposes to which an individual consented. Other obligations include those for purpose limitation, notification, access and correction, accuracy, protection, retention limitation, transfer limitation, and accountability. Public authorities cannot access data from private companies without meaningful safeguards (orders issued by public authority or courts). However, the disclosure of personal data to organizations and/or legal enforcement agencies without needing to obtain the consent of the individual is permitted under the PDPA in certain limited circumstances. State laws such as the Prevention of Corruption Act, the Telecommunications Act, the Criminal Procedure Code, and the Cybersecurity Act of 2018 may supersede the PDPA and allow organizations to collect or use data about an individual without the person’s consent where such collection is necessary for any investigation or proceedings, so as not to compromise the availability or accuracy of the personal data with or without a court order. Furthermore, public agencies are governed by government instruction manuals as well as legislation such as the Public Sector (Governance) Act, the Police Force Act, and the Statutory Bodies and Government Companies (Protection of Secrecy) Act. These pieces of legislation as well as the government instruction manuals provide the framework within which public agencies are to disclose data and information to each other. They also require individuals working in public agencies to safeguard the secrecy and confidentiality of any information received and not to make unauthorized disclosures of the same.</p>
<p>Are there limitations on how third parties, including public authorities, can use the data they access?</p>	<p>Yes. Public and private authorities may only use the data they access or receive from third parties for justified and limited purposes – for example, in the case of public authorities, for law enforcement, protection of public health, and safeguarding national security. The PDPA states that the Personal Data Protection Commission (PDPC) may not share any information with a foreign data protection body unless there is an undertaking in writing that it will comply with its terms in respect to the disclosed data.</p>
<p>Do individuals have effective and enforceable rights and remedies in relation to the safeguards for third-party access?</p>	<p>Yes. There are clear and enforceable rights in place within the PDPA to allow individuals to withdraw consent to collection, use, and disclosure of personal data and to access to and correction of their personal data. Individuals who have suffered loss or damage (such as financial loss, damage to property, or personal injury, including psychiatric illness) directly arising from a contravention of the data protection provisions may obtain an injunction, declaration, damages, or any other relief against the errant organization in civil proceedings in court. However, no private action against the organization may be</p>

	taken until after the right of appeal has been exhausted and the final decision is made.
Is there effective oversight?	The PDPC is the key agency responsible for administering and enforcing the PDPA.
Does the destination country have mature data protection and/or privacy laws in place?	Singapore passed the PDPA in 2012, and it took effect in 2014. The PDPA is a generally applicable data protection law for private-sector actors that imposes notice and legal basis requirements as well as other fundamental data protection principles and is administered and enforced by the PDPC. There are also various sector-specific legislation, such as the Banking Act, the Telecommunications Act, the Education Act, and the Private Hospitals and Medical Clinics Act that impose specific data protection obligations. Recent approved amendments to the PDPA include the requirement of organizations to notify the PDPC within 72 hours of any data breach, newly defined offenses relating to egregious mishandling of personal data, higher financial penalties for noncompliance with the PDPA, and a new data portability right for individuals.
Is there a legal framework governing the use of biometrics or facial recognition?	No biometric data will be transferred to Singapore. There is no current law or legal framework governing the use of biometrics or facial recognition.
What other factors should be considered?	There is a history of respect for human rights (in particular, the rights to privacy, freedom of expression, and access to justice).