Erklärung zu Risiken und Auswirkungen der Datenübermittlung

24. Januar 2022

Übersicht

Die Datenschutzlandschaft ist dynamisch. UKG hat die Datenschutzgrundsätze der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) als Grundlage für unser Datenschutzprogramm übernommen. Diese Grundsätze bieten eine konsistente Grundlage für den Datenschutz bei Entwicklung und Betrieb der Produkte und Dienstleistungen von UKG und ermöglichen uns die Anpassung an Änderungen in der Datenschutzlandschaft, sobald sie auftreten.

Als Reaktion auf Schrems II und die Empfehlungen 2020/1 und 2020/2 stützt sich UKG auf Modul 2 der am 4. Juni 2021 verabschiedeten Standardvertragsklauseln (SCC) als Mechanismus, der die grenzüberschreitende Übermittlung personenbezogener Daten zwischen der EU und Staaten ermöglicht, die weder Mitglieder des Europäischen Wirtschaftsraums (EWR) sind noch von der EU gemäß Artikel 5 der DSGVO als angemessen eingestuft werden. UKG hat diese Standardvertragsklauseln in seinen Zusatz zum Datenschutz (Data Protection Addendum, DPA) aufgenommen.

Wenn wir die personenbezogenen Daten unserer Kunden verarbeiten, ist UKG Auftragsverarbeiter. UKG kann andere Auftragsverarbeiter (d. h. Unterverarbeiter) beauftragen, um die von unserem Kunden angeforderte Verarbeitung personenbezogener Daten zu ermöglichen, wie in unseren Kundenverträgen genauer festgelegt. UKG hat mit seinen Unterverarbeitern außerdem Vereinbarungen getroffen, die schriftliche Zusicherungen umfassen, welche die konsistente und angemessene Verarbeitung und den Schutz von personenbezogenen Daten sicherstellen sollen. Kunden finden zusätzliche Informationen über unseren Einsatz von Unterverarbeitern in ihrer Kundenvereinbarung mit uns und dem Nachtrag zum Datenschutz (DPA). Bitte beachten Sie die nachstehenden entsprechenden Links für produktspezifische Informationen über unseren Umgang mit personenbezogenen Daten und unsere Sicherheitsvorkehrungen.

UKG ist der Ansicht, dass ein Kunde die Kontrolle über die Informationen haben sollte, die über seine Mitarbeiter gesammelt, erstellt, kommuniziert und gespeichert werden. UKG gewährt keiner anderen Person Zugang zu den Informationen eines Kunden, es sei denn, der Kunde weist uns dazu an, erteilt seine Zustimmung, oder wir sind gesetzlich dazu verpflichtet. UKG unterstützt keinen direkten Hintertür-Zugang auf seine Operationen (einschließlich unserer Datenspeicher) durch eine Regierung. UKG gibt seine Verschlüsselungsschlüssel nicht weiter und bietet auch keine Möglichkeit der Weitergabe seiner Verschlüsselungsschlüssel an eine Regierung.

Als Auftragsverarbeiter verschlüsselt UKG personenbezogene Daten bei der Speicherung und Übermittlung. UKG beschränkt den Zugang zu seinen Verschlüsselungsschlüsseln und verschlüsselt sie. UKG unterstützt nicht die Funktion „Bring Your Own Key“ (BYOK) für seine Kunden. UKG unterhält seine Datenschutz- und Sicherheitsprogramme in Übereinstimmung mit seinen Kundenvereinbarungen. Dazu gehören unser Zusatz zum Datenschutz (DPA) und unser Sicherheitsnachtrag, die unsere Programme und Praktiken in Bezug auf Datenschutz und Datensicherheit beschreiben. Abhängig vom gekauften Produkt und den vom Kunden verwendeten Anwendungen unterhält UKG Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2. Bitte beachten Sie die nachstehenden entsprechenden Links für produktspezifische Sicherheitszertifizierungen.

Ergebniserklärung

Basierend auf den Informationen in dieser Erklärung hat UKG entschieden, dass es mit der Übermittlung personenbezogener Daten aus dem EWR in Länder außerhalb des EWR (allgemein als Drittländer bezeichnet) fortfahren kann. Die Übermittlung personenbezogener Daten aus dem EWR an Drittländer durch UKG unterliegt den Standardvertragsklauseln (SCC). Die darin auferlegten Verpflichtungen sollen sicherstellen, dass den personenbezogenen Daten aus dem EWR, die an Drittländer übermittelt werden, ein Schutzniveau gewährt wird, das im Wesentlichen gleichwertig ist mit dem in der Europäischen Union (EU) und/oder dem Vereinigten Königreich garantierten Schutzniveau. Darüber hinaus hat UKG keinen Grund zu der Annahme, dass Gesetze, die in den Drittländern bestehen, in die es die personenbezogenen Daten übermittelt, in der Praxis so ausgelegt und/oder angewendet werden, dass die Übermittlung personenbezogener EWR-Daten durch UKG an diese Drittländer erfasst wird.

Inhaltsverzeichnis

Produktspezifische Informationen

UKG Dimensions

UKG Dimensions			
Wo befindet sich der Importeur?	USA	INDIEN	AUSTRALIEN
Leitet der Importeur die Daten an eine andere Organisation weiter?	Ja	Nein	Nein
Falls ja, um welche Art von Organisation handelt es sich und wo befindet sie sich?	UKG Dimensions – Unterverarbeiter	n. zutr.	n. zutr.
Warum führen Sie die Übermittlung durch?	Eine grenzüberschreitende Übermittlung ist für das Kunden-Onboarding und den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.
Was wird der Importeur (und jede andere Partei, an die er die Daten weiterleitet) mit den personenbezogenen Daten tun?	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um das Onboarding von Kunden durchzuführen und Kundensupport bereitzustellen.	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um Kundensupport bereitzustellen.	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um Kundensupport bereitzustellen.
Welche Sicherheitszertifizierungen unterhält UKG?	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie

	Berichte nach SOC 1 und SOC 2.	Berichte nach SOC 1 und SOC 2.	Berichte nach SOC 1 und SOC 2.
Auf wen beziehen sich die Daten?	Mitarbeiter	Mitarbeiter	Mitarbeiter
Welche Art(en) von Daten werden übermittelt?	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.
Wie werden die Daten gesendet?	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.
Wie lange ist der Zugriff auf die Daten durch den Importeur (und andere Empfänger) möglich?	Der Zugang zu personenbezogenen Daten basiert auf rollenbezogenen Berechtigungen, die nach dem Need-to-know-Prinzip zugewiesen werden. Die Aufbewahrung personenbezogener Daten wird vom Kunden festgelegt. Der Zugriff auf Kundendaten ist nur erforderlich, bis die Implementierung des Kunden oder bis die Supportanfrage des Kunden abgeschlossen ist.	Der Zugang zu personenbezogenen Daten basiert auf rollenbezogenen Berechtigungen, die nach dem Need-to-know-Prinzip zugewiesen werden. Nur Lesezugriff ist möglich. Auf personenbezogene Daten kann von Indien aus zugegriffen werden, sie werden jedoch nicht in Indien gespeichert oder aufbewahrt. Der Zugriff auf Kundendaten ist nur erforderlich, bis die Supportanfrage des Kunden abgeschlossen ist.	Der Zugang zu personenbezogenen Daten basiert auf rollenbezogenen Berechtigungen, die nach dem Need-to-know-Prinzip zugewiesen werden. Nur Lesezugriff ist möglich. Auf personenbezogene Daten kann von Australien aus zugegriffen werden, sie werden jedoch nicht in Australien gespeichert oder aufbewahrt. Der Zugriff auf Kundendaten ist nur erforderlich, bis die Supportanfrage des Kunden abgeschlossen ist.

Wie häufig werden diese Übermittlungen durchgeführt?	Grenzüberschreitende Übermittlungen für Onboarding-Zwecke erfolgen in der Implementierungsphase der Dienstleistung. Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.	Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.	Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.

UKG Pro

UKG Pro		
Wo befindet sich der Importeur?	USA	SINGAPUR
Leitet der Importeur die Daten an eine andere Organisation weiter?	Nein	Nein
Warum führen Sie die Übermittlung durch?	Eine grenzüberschreitende Übermittlung ist für das Kunden-Onboarding und den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.
Was wird der Importeur (und jede andere Partei, an die er die Daten weiterleitet) mit den personenbezogenen Daten tun?	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um das Onboarding von Kunden durchzuführen und Kundensupport bereitzustellen.	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um Kundensupport bereitzustellen.
Welche Sicherheitszertifizierungen unterhält UKG?	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.

Auf wen beziehen sich die Daten?	Personenbezogene Daten können Mitarbeiter und ehemalige Mitarbeiter des Kunden betreffen.	Personenbezogene Daten können Mitarbeiter und ehemalige Mitarbeiter des Kunden betreffen.
Welche Art(en) von Daten werden übermittelt?	Die übermittelten Daten dienen nur für Zwecke der Sicherheitsanalyse: Protokolldaten, Anmeldeinformationen, IP-Adressen, Mitarbeiter-IDs, Firmenname, Kontonummern, Banknamen, Bankleitzahlen.	Die übermittelten Daten dienen nur für Zwecke der Sicherheitsanalyse: Protokolldaten, Anmeldeinformationen, IP-Adressen, Mitarbeiter-IDs, Firmenname, Kontonummern, Banknamen, Bankleitzahlen.
Wie werden die Daten gesendet?	Der Fernzugriff auf die Daten kann über VPN-, SSL- und AES-256-Bit-Verschlüsselung erfolgen. Auch das Senden der Daten kann verschlüsselt über SFTP, PGP, SSL oder TLS erfolgen.	Der Fernzugriff auf die Daten kann über VPN-, SSL- und AES-256-Bit-Verschlüsselung erfolgen. Auch das Senden der Daten kann verschlüsselt über SFTP, PGP, SSL oder TLS erfolgen.
Wie lange ist der Zugriff auf die Daten durch den Importeur (und andere Empfänger) möglich?	UKG und seine Unterverarbeiter verarbeiten personenbezogene Daten nur wie angewiesen und wie in der Vereinbarung mit dem Kunden beschrieben, um geltende Gesetze einzuhalten oder für andere berechtigte Interessen.	UKG und seine Unterverarbeiter verarbeiten personenbezogene Daten nur wie angewiesen und wie in der Vereinbarung mit dem Kunden beschrieben, um geltende Gesetze einzuhalten oder für andere berechtigte Interessen.
Wie häufig werden diese Übermittlungen durchgeführt?	Übermittlungen erfolgen entsprechend der vereinbarten Erbringung von Dienstleistungen, die in der vertraglichen Verpflichtung von UKG mit dem Kunden aufgeführt sind, oder auf Anweisung des Kunden.	Übermittlungen erfolgen entsprechend der vereinbarten Erbringung von Dienstleistungen, die in der vertraglichen Verpflichtung von UKG mit dem Kunden aufgeführt sind, oder auf Anweisung des Kunden.

UKG Ready

UKG Ready			
Wo befindet sich der Importeur?	USA	INDIEN	AUSTRALIEN
Leitet der Importeur die Daten an eine andere Organisation weiter?	Nein	Nein	Nein
Warum führen Sie die Übermittlung durch?	Eine grenzüberschreitende Übermittlung ist für das Kunden-Onboarding und den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.
Was wird der Importeur (und jede andere Partei, an die er die Daten weiterleitet) mit den personenbezogenen Daten tun?	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um das Onboarding von Kunden durchzuführen und den Kunden bei der Problembehebung zu unterstützen.	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um den Kunden bei der Problembehebung zu unterstützen.	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um den Kunden bei der Problembehebung zu unterstützen.
Welche Sicherheitszertifizierungen unterhält UKG?	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.
Auf wen beziehen sich die Daten?	Mitarbeiter	Mitarbeiter	Mitarbeiter

Welche Art(en) von Daten werden übermittelt?	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.
Wie werden die Daten gesendet?	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.
Wie lange ist der Zugriff auf die Daten durch den Importeur (und andere Empfänger) möglich?	Support- und Professional Services-Mitarbeiter besitzen im Bedarfsfall „SA“ (Systemadministrator)-Zugriff auf ein Kundenkonto. Diese Konten auf Administratorebene bieten nur Lesezugriff. Der Zugriff wird den Support-Mitarbeitern nur im Bedarfsfall gewährt. Dies gilt in erster Linie für EU-Support-Mitarbeiter. Danach werden weitere Benutzer aus den US-amerikanischen Supportteams nur zu denen hinzugefügt, die Zugriff für weitere/überlaufende Supportressourcen oder Second- bzw. Third-Tier-Support (d. h. Lösungen/Shared Services) benötigen.	Support- und Professional Services-Mitarbeiter besitzen „SA“ (Systemadministrator)-Zugriff auf ein Kundenkonto. Diese Konten auf Administratorebene bieten nur Lesezugriff. Der Zugriff wird den Support-Mitarbeitern nur im Bedarfsfall gewährt. Dies gilt in erster Linie für EU-Support-Mitarbeiter. Danach werden weitere Benutzer aus den US-amerikanischen, indischen und australischen Supportteams nur zu denen hinzugefügt, die Zugriff für weitere/überlaufende Supportressourcen oder Second- bzw. Third-Tier-Support (d. h. Lösungen/Shared Services) benötigen.	Support- und Professional Services-Mitarbeiter besitzen „SA“ (Systemadministrator)-Zugriff auf ein Kundenkonto. Diese Konten auf Administratorebene bieten nur Lesezugriff. Der Zugriff wird den Support-Mitarbeitern nur im Bedarfsfall gewährt. Dies gilt in erster Linie für EU-Support-Mitarbeiter. Danach werden weitere Benutzer aus den US-amerikanischen, indischen und australischen Supportteams nur zu denen hinzugefügt, die Zugriff für weitere/überlaufende Supportressourcen oder Second- bzw. Third-Tier-Support (d. h. Lösungen/Shared Services) benötigen.

Wie häufig werden diese Übermittlungen durchgeführt?	Grenzüberschreitende Übermittlungen für Onboarding-Zwecke erfolgen in der Implementierungsphase der Dienstleistung. Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.	Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.	Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.

UKG Workforce Central

UKG Workforce Central			
Wo befindet sich der Importeur?	USA	INDIEN	AUSTRALIEN
Leitet der Importeur die Daten an eine andere Organisation weiter?	Ja	Nein	Nein
Um welche Art von Organisation handelt es sich und wo befindet sie sich?	UKG Workforce Central – Unterverarbeiter	n. zutr.	n. zutr.
Warum führen Sie die Übermittlung durch?	Eine grenzüberschreitende Übermittlung ist für das Kunden-Onboarding und den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.
Was wird der Importeur (und jede andere Partei, an die er die Daten weiterleitet) mit den	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen

personenbezogenen Daten tun?	Daten, um das Onboarding von Kunden durchzuführen und den Kunden bei der Problembehebung zu unterstützen.	Daten, um den Kunden bei der Problembehebung zu unterstützen.	Daten, um den Kunden bei der Problembehebung zu unterstützen.
Welche Sicherheitszertifizierungen unterhält UKG?	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.
Auf wen beziehen sich die Daten?	Mitarbeiter	Mitarbeiter	Mitarbeiter
Welche Art(en) von Daten werden übermittelt?	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit Human Capital Management und andere Daten, wie vom Kunden festgelegt.
Wie werden die Daten gesendet?	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.
Wie lange ist der Zugriff auf die Daten durch den Importeur (und andere Empfänger) möglich?	Support- und Professional Services-Mitarbeiter greifen über ein Set von Support-Konten – ADM und Ops – auf das System des Kunden zu. Das ADM-Konto verfügt über vollständige Administratorrechte, während das Ops-Konto über grundlegende Administratorrechte verfügt (nur Lese- und Schreibzugriff). Beide Konten bieten – bei	Support- und Professional Services-Mitarbeiter greifen über ein Set von Support-Konten – ADM und Ops – auf das System des Kunden zu. Das ADM-Konto verfügt über vollständige Administratorrechte, während das Ops-Konto über grundlegende Administratorrechte verfügt (nur Lese- und Schreibzugriff). Beide Konten bieten – bei	Support- und Professional Services-Mitarbeiter greifen über ein Set von Support-Konten – ADM und Ops – auf das System des Kunden zu. Das ADM-Konto verfügt über vollständige Administratorrechte, während das Ops-Konto über grundlegende Administratorrechte verfügt (nur Lese- und Schreibzugriff). Beide Konten bieten – bei

	Aktivierung – Zugriff auf alle Mitarbeiterdaten, außer bei Erweiterungen für Gesundheitskunden. Diese Daten sind für UKG-Mitarbeiter nicht sichtbar. Der Zugriff auf das Verschlüsselungs-Gateway des Kunden ist erforderlich, um Kundendaten anzuzeigen. Der Zugriff auf Daten eines Kunden ist nur erforderlich, bis die Implementierung des Kunden oder die Supportanfrage des Kunden abgeschlossen ist und die Daten gemäß interner Verfahren nicht mehr benötigt werden.	Aktivierung – Zugriff auf alle Mitarbeiterdaten, außer bei Erweiterungen für Gesundheitskunden. Diese Daten sind für UKG-Mitarbeiter nicht sichtbar. Der Zugriff auf das Verschlüsselungs-Gateway des Kunden ist erforderlich, um Kundendaten anzuzeigen. Der Zugriff auf die Daten eines Kunden ist nur erforderlich, bis die Support-Anfrage des Kunden abgeschlossen ist und die Daten gemäß interner Verfahren nicht mehr benötigt werden.	Aktivierung – Zugriff auf alle Mitarbeiterdaten, außer bei Erweiterungen für Gesundheitskunden. Diese Daten sind für UKG-Mitarbeiter nicht sichtbar. Der Zugriff auf das Verschlüsselungs-Gateway des Kunden ist erforderlich, um Kundendaten anzuzeigen. Der Zugriff auf die Daten eines Kunden ist nur erforderlich, bis die Support-Anfrage des Kunden abgeschlossen ist und die Daten gemäß interner Verfahren nicht mehr benötigt werden.
Wie häufig werden diese Übermittlungen durchgeführt?	Grenzüberschreitende Übermittlungen für Onboarding-Zwecke erfolgen in der Implementierungsphase der Dienstleistung. Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.	Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.	Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.

UKG HR Service Delivery

UKG HR Service Delivery		
Wo befindet sich der Importeur?	USA	INDIEN
Leitet der Importeur die Daten an eine andere Organisation weiter?	Ja	Nein
Falls ja, um welche Art von Organisation handelt es sich und wo befindet sie sich?	HR Service Delivery – Unterverarbeiter	n. zutr.
Warum führen Sie die Übermittlung durch?	Eine grenzüberschreitende Übermittlung ist für das Kunden-Onboarding und den Kundensupport erforderlich.	Eine grenzüberschreitende Übermittlung ist für den Kundensupport erforderlich.
Was wird der Importeur (und jede andere Partei, an die er die Daten weiterleitet) mit den personenbezogenen Daten tun?	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um das Onboarding von Kunden durchzuführen und den Kunden bei der Problembehebung zu unterstützen.	Der Empfänger nutzt die Verarbeitung (Speicherung, Zugriff, Bearbeitung und Aufbewahrung) von personenbezogenen Daten, um den Kunden bei der Problembehebung zu unterstützen.
Welche Sicherheitszertifizierungen unterhält UKG?	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.	UKG unterhält Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27018 sowie Berichte nach SOC 1 und SOC 2.
Auf wen beziehen sich die Daten?	Mitarbeiter, Vertreter, Subunternehmer, Berater, Fachexperten und Ansprechpartner.	Mitarbeiter, Vertreter, Subunternehmer, Berater, Fachexperten und Ansprechpartner.
Welche Art(en) von Daten werden übermittelt?	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit	Das Produkt verarbeitet personenbezogene Daten im Zusammenhang mit

	Human Capital Management-Daten.	Human Capital Management-Daten.
Wie werden die Daten gesendet?	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.	Die Daten werden verschlüsselt per SFTP oder TLS gesendet.
Wie lange ist der Zugriff auf die Daten durch den Importeur (und andere Empfänger) möglich?	UKG und seine Unterverarbeiter verarbeiten personenbezogene Daten nur wie angewiesen und wie in der Vereinbarung mit dem Kunden beschrieben, um geltende Gesetze einzuhalten oder für andere berechtigte Interessen.	Support- und Professional Services-Mitarbeiter besitzen „SA“ (Systemadministrator)-Zugriff auf ein Kundenkonto. Diese Konten auf Administratorebene bieten nur Lesezugriff. Der Zugang wird nur im Bedarfsfall gewährt.
Wie häufig werden diese Übermittlungen durchgeführt?	Übermittlungen erfolgen entsprechend der vereinbarten Erbringung von Dienstleistungen, die in der vertraglichen Verpflichtung von UKG mit dem Kunden aufgeführt sind, oder auf Anweisung des Kunden.	Grenzüberschreitende Übermittlungen für Supportzwecke erfolgen episodisch je nach Bedarf des Kunden.

Landesspezifische Informationen

USA

USA	
Sind die vertraglichen Schutzmechanismen im Bestimmungsland durchsetzbar?	Ja. Die USA erkennen die Rechtsstaatlichkeit an, da ein etabliertes und respektiertes Rechts- und Gerichtssystem vorhanden ist. Ausländische Urteile oder Schiedssprüche können vollstreckt werden. Nach US-amerikanischem Recht muss eine Person, die die Vollstreckung eines ausländischen Urteils, Dekrets oder einer Anordnung in den USA erreichen möchte, bei einem zuständigen Gericht Klage erheben. Das Gericht entscheidet dann, ob das ausländische Urteil anerkannt und vollstreckt wird. Die USA sind seit dem 15. Oktober 1964 Mitglied der Haager Konferenz für Internationales Privatrecht und gehören zu den Vertragsstaaten von sechs Übereinkommen der Haager Konferenz, darunter das Gerichtsstandsübereinkommen. Das Gerichtssystem, das Mittel für Wiedergutmachung und wirksame Rechtsbehelfe bereitstellt, bietet einen einfachen Zugang zur Justiz. Die Rechte von Drittbegünstigten aus Verträgen werden anerkannt und durchgesetzt. Gerichtsverfahren weisen ein hohes Maß an Integrität und Unabhängigkeit auf. Das Vereinigte Königreich prüft derzeit die Möglichkeit, in Bezug auf die Datenschutzbestimmungen der USA auf Angemessenheit zu befinden.
Gibt es Gesetze, die festlegen, wann und wie gesetzlich verlangt werden kann, dass Dritten, einschließlich Behörden, Zugang zu Daten gewährt wird?	Ja. Behörden oder Dritte können ohne sinnvolle Sicherheitsvorkehrungen (z. B. Gerichtsbeschluss oder Haftbefehl) nicht auf Daten von Privatunternehmen zugreifen, dazu gehört auch das Abfangen von Kommunikation. Organisationen können eine Arbeitsplatzüberwachung durchführen, es gibt jedoch erhebliche Schutzmechanismen.
Gibt es Einschränkungen dafür, wie Dritte, einschließlich Behörden, die Daten verwenden können, auf die sie zugreifen?	Ja. Öffentliche und private Behörden dürfen die Daten, auf die sie zugreifen oder die sie von Dritten erhalten, nur für berechtigte und begrenzte Zwecke verwenden – beispielsweise im Fall von Behörden zur Strafverfolgung, zum Schutz der öffentlichen Gesundheit und zur Wahrung der nationalen Sicherheit.

Haben Einzelpersonen wirksame und durchsetzbare Rechte und Rechtsbehelfe in Bezug auf die Sicherheitsvorkehrungen gegen den Zugriff Dritter?	Ja. Es sind klare und durchsetzbare Rechte vorhanden, um Einzelpersonen den Zugriff auf ihre personenbezogenen Daten zu gewähren. Des Weiteren können Einzelpersonen ohne Weiteres den Zugriff durch private und öffentliche Behörden auf ihre Daten, auch durch den Einsatz von Überwachungsmaßnahmen, gerichtlich anfechten.
Gibt es eine wirksame Aufsicht?	Ja. Polizei und Geheimdienste arbeiten unter klarer gerichtlicher oder anderer wirksamer Verwaltungsaufsicht über ihre Aktivitäten.
Verfügt das Zielland über einen ausgereiften Datenschutz und/oder Datenschutzgesetze?	Die US-amerikanische Verfassung geht nicht ausdrücklich auf die Privatsphäre des Einzelnen ein. Der Oberste Gerichtshof der USA hat in seinen Entscheidungen unter Berufung auf den ersten, dritten, vierten, fünften und neunten Zusatzartikel zur Verfassung ein Recht auf Privatsphäre abgeleitet. Anstelle einer bundesweiten Datenschutzgesetzgebung gibt es in den USA einen Flickenteppich von sektorspezifischen Datenschutzgesetzen und -vorschriften, die die Verarbeitung personenbezogener Daten einschränken. Diese Gesetze betreffen Informationen über die Steuern einer Einzelperson (IRS-Regeln), Verbraucherkredite (FCRA), Finanzkonten (GLBA), Bildungsaufzeichnungen (FERPA), Gesundheitsinformationen (HIPAA) und dergleichen mehr. Die US Federal Trade Commission (FTC) führt seit fast 50 Jahren Datenschutz- und Sicherheitsmaßnahmen im Rahmen des FCRA (Fair Credit Reporting Act, Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten) und in jüngerer Zeit auch im Rahmen der Programme „Safe Harbor“ und „Privacy Shield“ durch. Die FTC ergreift außerdem Maßnahmen wegen unlauterer oder irreführender Handelspraktiken gegen Unternehmen, wenn die Verarbeitung personenbezogener Daten nicht mit ihrer Datenschutzerklärung vereinbar ist. Darüber hinaus sind alle US-Bundesstaaten und Protektorate befugt, eigene Gesetze und Vorschriften zum Schutz der Privatsphäre und des Datenschutzes zu erlassen. Viele bundesstaatliche Gesetze sind auf den Verbraucherschutz fokussiert. Die Auswirkungen dieser Gesetze können jedoch recht weitreichend sein, wie z. B. die Anwendung der kalifornischen Gesetze CCPA (California Consumer Privacy Act) und CPRA (Consumer Privacy Rights Act) auf personenbezogene Daten, die im Beschäftigungskontext erhoben werden. Der Flickenteppich von Gesetzen auf Bundes- und Bundesstaatenebene bildet in Kombination mit abgeleiteten Bestimmungen zum Schutz der

	Verfassung einen Rahmen für den Schutz personenbezogener Daten.
Gibt es einen rechtlichen Rahmen für die Verwendung von Biometrie oder Gesichtserkennung?	In den USA werden biometrische Erkennung und Gesichtserkennung nicht auf nationaler Ebene behandelt. Nicht alle Bundesstaaten haben Gesetze, die sich mit diesen Angelegenheiten befassen, und bei denen, die dies tun, gibt es Unterschiede.
Welche anderen Faktoren sollten berücksichtigt werden?	Die Menschenrechte (insbesondere das Recht auf Privatsphäre, das Recht auf Meinungsfreiheit und das Recht auf Zugang zur Justiz) werden allgemein beachtet.

AUSTRALIEN

AUSTRALIEN	
Sind die vertraglichen Schutzmechanismen im Bestimmungsland durchsetzbar?	Ja. Australien erkennt die Rechtsstaatlichkeit an, da ein etabliertes und respektiertes Rechts- und Gerichtssystem vorhanden ist. Ausländische Urteile oder Schiedssprüche können vollstreckt werden. Die Vollstreckung ausländischer Urteile in Australien unterliegt sowohl gesetzlichen Regelungen als auch den Grundsätzen des Common Law. In Bezug auf gesetzliche Regelungen sehen der Foreign Judgments Act 1991 und die Foreign Judgments Regulations 1992 ein Verfahren und einen Geltungsbereich der Urteile vor, die im Rahmen der gesetzlichen Regelungen vollstreckbar sind. Darüber hinaus ist Australien zusammen mit dem Vereinigten Königreich Vertragspartei des bilateralen Abkommens über die gegenseitige Anerkennung und Vollstreckung von gerichtlichen Entscheidungen in Zivil- und Handelssachen von 1994. Australien ist jedoch nicht Vertragspartei des Haager Übereinkommens über die Anerkennung und Vollstreckung ausländischer Urteile in Zivil- und Handelssachen von 1971. In Fällen, in denen keine internationale oder gesetzliche Vereinbarung besteht, muss ein ausländisches Urteil nach den Grundsätzen des Common Law vollstreckt werden.
Gibt es Gesetze, die festlegen, wann und wie gesetzlich verlangt	Ja. Behörden oder Dritte können ohne wirkungsvolle Sicherheitsvorkehrungen (z. B. Gerichtsbeschluss oder

werden kann, dass Dritten, einschließlich Behörden, Zugang zu Daten gewährt wird?	Haftbefehl) nicht auf Daten von Privatunternehmen zugreifen, dazu gehört auch das Abfangen von Kommunikation. Organisationen können Arbeitsplatzüberwachung durchführen, aber es gibt erhebliche Schutzmechanismen.
Gibt es Einschränkungen dafür, wie Dritte, einschließlich Behörden, die Daten verwenden können, auf die sie zugreifen?	Ja. Öffentliche und private Behörden dürfen die Daten, auf die sie zugreifen oder die sie von Dritten erhalten, nur für berechtigte und begrenzte Zwecke verwenden. Beispielsweise im Fall von Behörden zur Strafverfolgung zum Schutz der öffentlichen Gesundheit und zur Wahrung der nationalen Sicherheit.
Haben Einzelpersonen wirksame und durchsetzbare Rechte und Rechtsbehelfe in Bezug auf die Sicherheitsvorkehrungen gegen den Zugriff Dritter?	Ja. Es sind klare und durchsetzbare Rechte vorhanden, um Einzelpersonen den Zugriff auf ihre personenbezogenen Daten zu gewähren. Des Weiteren können Einzelpersonen ohne Weiteres den Zugriff durch private und öffentliche Behörden auf ihre Daten, auch durch den Einsatz von Überwachungsmaßnahmen, gerichtlich anfechten.
Gibt es eine wirksame Aufsicht?	Ja. Polizei und Geheimdienste arbeiten unter klarer gerichtlicher oder anderer wirksamer Verwaltungsaufsicht über ihre Aktivitäten.
Verfügt das Zielland über einen ausgereiften Datenschutz und/oder Datenschutzgesetze?	Datensicherheit und Datenschutz werden in Australien durch eine Kombination von Gesetzen auf Bundes-, Bundesstaaten- und Territorialebene geregelt. Der Privacy Act 1988 (Cth), der die Australian Privacy Principles (APPs) enthält, ist zentral für die Datenschutzgesetzgebung in Australien. Der Privacy Act gilt für Unternehmen der Privatwirtschaft (mit einem Jahresumsatz von mehr als 3 Mio. AUD) sowie alle Regierungsbehörden des Commonwealth und andere spezifische Unternehmen, die die Umsatzschwellen nicht erfüllen, darunter private Gesundheitsdienstleister, die Gesundheitsinformationen verarbeiten, Kreditauskunfteien und Unternehmen, die personenbezogene Daten verkaufen oder kaufen (APP-Unternehmen). Die meisten Bundesstaaten und Territorien haben außerdem ihre eigenen (grob aufeinander abgestimmten) Datenschutzgesetze, die für staatliche Regierungsbehörden und private Unternehmen gelten, die mit ihnen Verträge abschließen. Neben dem Privacy Act, den Australian Privacy Principles (APPs) und den bundesstaatlichen Datenschutzgesetzen gibt es auch spezifische sektorfokussierte Gesetze, die Datenschutz- und Datenrisiken regeln, beispielsweise im Gesundheitssektor und im Telekommunikationssektor. Es gibt außerdem weitere Gesetze

	auf Ebene des Commonwealth und der Bundesstaaten, die für den Datenschutz und die Verwendung personenbezogener Daten relevant sind, darunter der Spam Act 2003 (Cth), der Do Not Call Register Act 2006 (Cth) und Strafgesetze, die den unbefugten Zugriff auf Computersysteme verbieten, sowie verschiedene Gesetze zu Überwachungs- und Abhörgeräten. In jüngerer Zeit wurde mit dem Treasury Laws Amendment (Consumer Data Right) Act 2019 ein verbraucherorientierter Mechanismus der Datenübertragbarkeit eingeführt, der derzeit für den Bankensektor gilt. Darüber hinaus haben bestimmte Regulierungsbehörden (nicht gesetzlich vorgeschriebene/nicht obligatorische) Standards herausgegeben, die regulierten Unternehmen Vorgaben in Bezug auf definierte Datenschutzmaßnahmen in die Hand geben, die ergriffen werden sollten. Die australische Regulierungsbehörde Australian Prudential and Regulatory Authority (APRA) beispielsweise reguliert Finanzdienstleistungsinstitute und hat eine Reihe von „aufsichtsrechtlichen" Standards zu Datenschutz- und Datenrisiken eingeführt. Letztendlich verbietet das Australian Consumer Law (ACL) entsprechenden Unternehmen (darunter digitale Plattformen), die in Australien Geschäfte tätigen, bestimmte Verhaltensweisen im Zusammenhang mit der Lieferung oder dem Erwerb von Waren oder Dienstleistungen. Dazu gehören irreführendes oder täuschendes Verhalten, gewissenloses Verhalten und unlautere Praktiken. Jedes dieser Verbote unter dem Australian Consumer Law (ACL) wurde kürzlich von der Australian Competition and Consumer Commission (ACCC) (als Regulierungsbehörde) als anwendbar auf die Datenschutzpraktiken einer Organisation angeführt, einschließlich von Erklärungen und Aussagen darüber, wie Benutzerdaten gesammelt und offengelegt werden, auch im Rahmen von Datenschutzrichtlinien und Nutzungsbedingungen.
Gibt es einen rechtlichen Rahmen für die Verwendung von Biometrie oder Gesichtserkennung?	In Australien regelt der Privacy Act 1988 (Cth) die Art und Weise, wie personenbezogene Daten, einschließlich biometrischer Daten, erfasst und verwendet werden.
Welche anderen Faktoren sollten berücksichtigt werden?	Die Menschenrechte (insbesondere das Recht auf Privatsphäre, das Recht auf Meinungsfreiheit und das Recht auf Zugang zur Justiz) werden allgemein beachtet.

INDIEN

INDIEN	
Sind die vertraglichen Schutzmechanismen im Bestimmungsland durchsetzbar?	Ja. Indien erkennt die Rechtsstaatlichkeit an, da ein etabliertes und respektiertes Rechts- und Gerichtssystem vorhanden ist. In Indien können Urteile von Gerichten in „Territorien im Gegenseitigkeitsverhältnis“ direkt durch Einreichung bei einem indischen Gericht und Vollstreckungsdekret vollstreckt werden. Indien ist Mitglied der Haager Konferenz. Das Gerichtssystem, das Mittel für Wiedergutmachung und wirksame Rechtsbehelfe bereitstellt, bietet einen einfachen Zugang zur Justiz. Die Rechte von Drittbegünstigten aus Verträgen werden anerkannt und durchgesetzt. Gerichtsverfahren weisen ein hohes Maß an Integrität und Unabhängigkeit auf. Das Vereinigte Königreich prüft derzeit die Möglichkeit, in Bezug auf die Datenschutzbestimmungen Indiens auf Angemessenheit zu befinden.
Gibt es Gesetze, die festlegen, wann und wie gesetzlich verlangt werden kann, dass Dritten, einschließlich Behörden, Zugang zu Daten gewährt wird?	Ja. Behörden oder Dritte können ohne wirkunsvolle Sicherheitsvorkehrungen (z. B. Gerichtsbeschluss oder Haftbefehl) nicht auf Daten von Privatunternehmen zugreifen, dazu gehört auch das Abfangen von Kommunikation. Organisationen können eine Arbeitsplatzüberwachung durchführen, es gibt jedoch erhebliche Schutzmechanismen.
Gibt es Einschränkungen dafür, wie Dritte, einschließlich Behörden, die Daten verwenden können, auf die sie zugreifen?	Ja. Öffentliche und private Behörden dürfen die Daten, auf die sie zugreifen oder die sie von Dritten erhalten, nur für berechtigte und begrenzte Zwecke verwenden – beispielsweise im Fall von Behörden zur Strafverfolgung, zum Schutz der öffentlichen Gesundheit und zur Wahrung der nationalen Sicherheit.
Haben Einzelpersonen wirksame und durchsetzbare Rechte und Rechtsbehelfe in Bezug auf die Sicherheitsvorkehrungen gegen den Zugriff Dritter?	Ja. Es sind klare und durchsetzbare Rechte vorhanden, um Einzelpersonen den Zugriff auf ihre personenbezogenen Daten zu gewähren. Des Weiteren können Einzelpersonen ohne Weiteres den Zugriff durch private und öffentliche Behörden auf ihre Daten, einschließlich Überwachungsmaßnahmen, gerichtlich anfechten.

Gibt es eine wirksame Aufsicht?	Ja. Polizei und Geheimdienste arbeiten unter klarer gerichtlicher oder anderer wirksamer Verwaltungsaufsicht über ihre Aktivitäten.
Verfügt das Zielland über einen ausgereiften Datenschutz und/oder Datenschutzgesetze?	In Indien beruht der Datenschutz auf der Auslegung der indischen Verfassung (Artikel 21 impliziert die Privatsphäre als Grundrecht) sowie auf sektorspezifischen Datenschutzgesetzen und -vorschriften. Sektorale Gesetze behandeln den Umgang mit und den Schutz von personenbezogenen Daten, wobei der Schwerpunkt auf der Einschränkung der Vertraulichkeit bei der Verwendung der personenbezogenen Daten liegt. Die Artikelgesetzgebung, die Personal Data Protection (PDP) Bill, wurde 2019 eingeführt. Bei Inkrafttreten wird durch die Personal Data Protection (PDP) Bill Abschnitt 43A des Information Technology Act 2000 (IT-Gesetz) aufgehoben, der den Umgang mit personenbezogenen Daten und sensiblen personenbezogenen Daten behandelt und dem Einzelnen ähnliche Rechte wie in der DSGVO gewährt.
Gibt es einen rechtlichen Rahmen für die Verwendung von Biometrie oder Gesichtserkennung?	Erhebung, Speicherung und Verarbeitung biometrischer Daten werden durch die Informationstechnologie-Vorschriften des IT-Gesetzes geregelt, insbesondere durch die darauf beruhenden Regeln. Die Regeln der Informationstechnologie (Angemessene Sicherheitspraktiken und -verfahren sowie sensible personenbezogene Daten) von 2011 (Regeln zur Privatsphäre) legen die spezifischen Bedingungen fest, die den Umgang mit personenbezogenen Daten und sensiblen personenbezogenen Daten oder Informationen, einschließlich biometrischer Daten, regeln.
Welche anderen Faktoren sollten berücksichtigt werden?	Die Menschenrechte (insbesondere das Recht auf Privatsphäre, das Recht auf Meinungsfreiheit und das Recht auf Zugang zur Justiz) werden allgemein beachtet.

SINGAPUR

SINGAPUR	
Sind die vertraglichen Schutzmechanismen im Bestimmungsland durchsetzbar?	Ja. Singapur erkennt die Rechtsstaatlichkeit an, da ein etabliertes und respektiertes Rechts- und Gerichtssystem vorhanden ist. Ausländische Urteile oder Schiedssprüche können vollstreckt werden. Nach singapurischem Recht muss eine Person, die die Vollstreckung eines ausländischen Urteils, Dekrets oder einer Anordnung in Singapur erreichen möchte, bei einem zuständigen Gericht Klage erheben. Das Gericht entscheidet dann, ob das ausländische Urteil anerkannt und vollstreckt wird. Singapur ist seit dem 9. April 2014 Mitglied der Haager Konferenz für Internationales Privatrecht und gehört zu den Vertragsstaaten von vier Übereinkommen der Haager Konferenz, darunter das Gerichtsstandsübereinkommen. Singapur ist außerdem Vertragsstaat des New Yorker Schiedsübereinkommens über die Anerkennung und Vollstreckung ausländischer Schiedssprüche. Das Gerichtssystem, das Mittel für Wiedergutmachung und wirksame Rechtsbehelfe bereitstellt, bietet einen einfachen Zugang zur Justiz. Die Rechte von Drittbegünstigten aus Verträgen werden anerkannt und durchgesetzt. Gerichtsverfahren weisen ein hohes Maß an Integrität und Unabhängigkeit auf. Das Vereinigte Königreich prüft derzeit die Möglichkeit, in Bezug auf die Datenschutzbestimmungen Singapurs auf Angemessenheit zu befinden.
Gibt es Gesetze, die festlegen, wann und wie gesetzlich verlangt werden kann, dass Dritten, einschließlich Behörden, Zugang zu Daten gewährt wird?	Unter dem Personal Data Protection Act (PDPA) von 2012 sind Datenverantwortliche und Datenverarbeiter im Privatsektor direkt verpflichtet, die Zustimmungspflichten für die Zwecke der Erhebung, Verwendung oder Offenlegung personenbezogener Daten für Zwecke einzuhalten, denen eine Person zugestimmt hat. Weitere Verpflichtungen umfassen Zweckbeschränkung, Benachrichtigung, Zugriff und Berichtigung, Genauigkeit, Schutz, Beschränkung der Aufbewahrung, Beschränkung der Übertragung und Rechenschaftspflicht. Behörden können ohne wirkungsvolle Schutzmaßnahmen (behördliche oder gerichtliche Anordnungen) nicht auf Daten von Privatunternehmen zugreifen. Die Offenlegung personenbezogener Daten gegenüber Organisationen und/oder

	Strafverfolgungsbehörden ist jedoch, ohne dass die Zustimmung des Einzelnen eingeholt werden muss, unter bestimmten eingeschränkten Umständen im Rahmen des Personal Data Protection Act (PDPA) zulässig. Staatliche Gesetze wie das Korruptionspräventionsgesetz, das Telekommunikationsgesetz, die Strafprozessordnung und das Cybersicherheitsgesetz von 2018 können den Personal Data Protection Act (PDPA) aufheben und es Organisationen ermöglichen, Daten über eine Person ohne Zustimmung dieser Person zu erfassen oder zu verwenden, wenn eine solche Erfassung für eine Ermittlung oder ein Verfahren erforderlich ist, um die Verfügbarkeit oder Genauigkeit der personenbezogenen Daten mit oder ohne Gerichtsbeschluss nicht zu gefährden. Darüber hinaus unterliegen staatliche Stellen behördlichen Handlungsanleitungen sowie Gesetzen, wie z. B. dem Gesetz über den öffentlichen Sektor (Governance), dem Polizeigesetz und dem Gesetz über gesetzliche Körperschaften und staatliche Unternehmen (Schutz der Geheimhaltung). Diese Gesetze sowie die behördlichen Anleitungen geben den Rahmen vor, innerhalb dessen staatliche Stellen Daten und Informationen untereinander offenlegen müssen. Sie verlangen auch von Personen, die in staatlichen Stellen arbeiten, die Geheimhaltung und Vertraulichkeit aller erhaltenen Informationen zu wahren und diese nicht unbefugt offenzulegen.
Gibt es Einschränkungen dafür, wie Dritte, einschließlich Behörden, die Daten verwenden können, auf die sie zugreifen?	Ja. Öffentliche und private Behörden dürfen die Daten, auf die sie zugreifen oder die sie von Dritten erhalten, nur für berechtigte und begrenzte Zwecke verwenden – beispielsweise im Fall von Behörden zur Strafverfolgung, zum Schutz der öffentlichen Gesundheit und zur Wahrung der nationalen Sicherheit. Der Personal Data Protection Act (PDPA) legt fest, dass die Personal Data Protection Commission (PDPC) keine Informationen an eine ausländische Datenschutzbehörde weitergeben darf, es sei denn, es liegt eine schriftliche Zusage vor, dass sie den Bedingungen hinsichtlich der offengelegten Daten entsprechen wird.
Haben Einzelpersonen wirksame und durchsetzbare Rechte und Rechtsbehelfe in Bezug auf die Sicherheitsvorkehrungen gegen den Zugriff Dritter?	Ja. Im Rahmen des Personal Data Protection Act (PDPA) sind klare und durchsetzbare Rechte vorhanden, die es Einzelpersonen ermöglichen, ihre Einwilligung zu Erhebung, Verwendung und Offenlegung personenbezogener Daten zu widerrufen und auf ihre personenbezogenen Daten zuzugreifen und diese zu korrigieren. Personen, die Verluste

	oder Schäden erleiden (z. B. finanzielle Verluste, Schäden an Eigentum oder persönliche Schäden, einschließlich psychischer Erkrankung), die direkt aufgrund eines Verstoßes gegen die Datenschutzbestimmungen entstanden sind, können eine gerichtliche Verfügung, Vereinbarung, Schadensersatz oder ein anderes Rechtsmittel gegenüber der sich fehlverhaltenden Organisation in Zivilverfahren vor Gericht geltend machen. Es dürfen jedoch keine privaten Maßnahmen gegen die Organisation ergriffen werden, bis das Recht auf Berufung erschöpft ist und die endgültige Entscheidung getroffen wurde.
Gibt es eine wirksame Aufsicht?	Die Personal Data Protection Commission (PDPC) ist die wichtigste Behörde Singapurs, die für die Verwaltung und Durchsetzung des Personal Data Protection Act (PDPA) zuständig ist.
Verfügt das Zielland über einen ausgereiften Datenschutz und/oder Datenschutzgesetze?	Der Personal Data Protection Act (PDPA) wurde im Jahr 2012 in Singapur verabschiedet und ist 2014 in Kraft getreten. Der PDPA ist ein Datenschutzgesetz mit allgemeiner Gültigkeit für Akteure im Privatsektor, das Informationspflichten und Rechtsgrundlagen sowie weitere grundlegende Datenschutzprinzipien vorschreibt und von der Personal Data Protection Commission (PDPC) verwaltet und durchgesetzt wird. Darüber hinaus gibt es verschiedene sektorspezifische Gesetze, wie das Bankengesetz, das Telekommunikationsgesetz, das Bildungsgesetz und das Gesetz über private Krankenhäuser und Kliniken, die bestimmte Datenschutzverpflichtungen auferlegen. Zu den kürzlich genehmigten Änderungen des PDPA gehören: die Anforderung von Organisationen, die Personal Data Protection Commission (PDPC) innerhalb von 72 Stunden über eine Datenschutzverletzung zu informieren, neu festgelegte Straftaten in Bezug auf schwerwiegende Fälle des Missbrauchs von personenbezogenen Daten, höhere Geldstrafen für die Nichteinhaltung des PDPA und ein neues Recht auf Datenübertragbarkeit für Einzelpersonen.
Gibt es einen rechtlichen Rahmen für die Verwendung von Biometrie oder Gesichtserkennung?	Biometrische Daten werden nicht nach Singapur übermittelt. Ein aktuelles Gesetz oder Rechtsrahmen für die Verwendung von Biometrie oder Gesichtserkennung ist nicht vorhanden.
Welche anderen Faktoren sollten berücksichtigt werden?	Die Menschenrechte (insbesondere das Recht auf Privatsphäre, das Recht auf Meinungsfreiheit und das Recht auf Zugang zur Justiz) werden allgemein beachtet.