Datenschutz Anlage ("Anlage") zum Auftragsformular

1 Diese Datenschutz Anlage gilt in Verbindung mit dem Auftragsformular (einschließlich der Geschäftsbedingungen für Geschäftsreisen und/oder der Geschäftsbedingungen für Tagungs- und Veranstaltungsdienstleistungen) (zusammenfassend als "Vertrag" bezeichnet) zwischen Reed & Mackay Deutschland GmbH ("R&M") (eingetragen in Deutschland unter der Nummer HRB 30513) mit eingetragenem Sitz in Robert – Bosch Str. 32, 63303 Dreieic, und Ihnen, dem Kunden. Definierte Begriffe, die an anderer Stelle im Vertrag verwendet werden, haben die gleiche Bedeutung in dieser Anlage. Wenn R&M personenbezogene Daten als Auftragsverarbeiter im Auftrag des Kunden verarbeitet, ist R&M verpflichtet:

1.1 Die Daten nur zu verwenden, um:

(a) seine Verpflichtungen aus diesem Vertrag zu erfüllen und diese Daten gemäß den schriftlichen Anweisungen des Kunden zu verarbeiten; und/oder

(b) der Datenschutzgesetzgebung oder die Gesetze eines anderen Mitgliedstaates der Europäischen Union einzuhalten(vorausgesetzt, dass R&M den Kunden vor der entsprechenden Verarbeitung über diese Anforderung informiert (es sei denn, das entsprechende Gesetz verbietet eine solche Mitteilung));

1.2 vorbehaltlich der Absätze 2, 4 und 5 (einschließlich) dieser Anlage geeignete technische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, um die im Zusammenhang mit diesem Vertrag verarbeiteten personenbezogene Daten vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Änderung, unbefugter Weitergabe oder unbefugtem Zugriff zu schützen, und alle gemäß Artikel 32 des GDPR erforderlichen Maßnahmen zu ergreifen ("Sicherheit der Verarbeitung");

1.3 alle angemessenen Maßnahmen zu ergreifen, um die Zuverlässigkeit aller R&M-Mitarbeiter zu gewährleisten, die Zugang zu Daten haben, die im Zusammenhang mit diesem Vertrag verarbeitet werden, und sicherzustellen, dass alle diese R&M-Mitarbeiter an durchsetzbare Geheimhaltungspflichten gebunden sind;

1.4 unter Berücksichtigung der Art der Verarbeitung den Kunden durch geeignete technische und organisatorische Maßnahmen zu unterstützen, soweit dies möglich ist, um die Verpflichtung des Kunden zu erfüllen, auf Anfragen von betroffenen Personen zu reagieren, die ihre Rechte gemäß Kapitel III des GDPR ausüben;

1.5 den Kunden dabei zu unterstützen, die Einhaltung seiner Verpflichtungen gemäß Artikel 32 - 36 des GDPR ("Sicherheit der Verarbeitung", "Meldung einer Verletzung des Schutzes personenbezogener Daten ...", "Datenschutz-Folgenabschätzung" und "vorherige Konsultation") zu gewährleisten, wobei die Art der Verarbeitung und die R&M zur Verfügung stehenden Informationen berücksichtigt sind;

1.6 den Kunden unverzüglich, auf jeden Fall aber innerhalb von 48 Stunden nach Bekanntwerden einer Sicherheitsverletzung zu benachrichtigen, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum Zugriff auf Daten führt, die von R&M im Zusammenhang mit diesem Vertrag verarbeitet werden;

1.7 dem Kunden innerhalb einer angemessenen Frist nach Benachrichtigung des Kunden alle Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung der in dieser Anlage aufgeführten Verpflichtungen nachzuweisen, und Audits, einschließlich Sicherheitstests oder Inspektionen, die vom Kunden oder einem anderen vom Kunden beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen, vorausgesetzt, dass:

- solche Audits, Sicherheitstests und/oder Inspektionen nur bei einer (1) Gelegenheit innerhalb eines Zeitraums von zwölf (12) Monaten stattfinden,
- dass solche Audits, Sicherheitstests und/oder Inspektionen strikt auf die Vorkehrungen von R&M zur Einhaltung dieser Anlage beschränkt sind,
- solche Audits, Sicherheitstests und/oder Inspektionen während der normalen Geschäftszeiten durchgeführt werden,
- der Kunde (oder der betreffende Dritte, der ein solches Audit, einen solchen Sicherheitstest und/oder eine solche Inspektion durchführt) R&M mit angemessener Frist im Voraus schriftlich über ein solches Audit , einen solchen Sicherheitstest und/oder eine solche Inspektion informiert und
- der Umfang eines solchen Audits, eines solchen Sicherheitstests und/oder einer solchen Inspektion vor deren Beginn mit R&M vereinbart wird;

1.8 berechtigt zu sein, Daten außerhalb des Europäischen Wirtschaftsraums zu übermitteln, sofern angemessene Garantien gemäß der Datenschutzgesetzgebung vorhanden sind, einschließlich, aber nicht beschränkt auf die Fälle, in denen dies angemessen ist: (a) für die Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum, die EU-Standardvertragsklauseln

(Modul 2 - Vom Verantwortlichen zum Verarbeiter) dargelegt; (b) für die Übermittlung von Daten aus dem Vereinigten Königreich, das UK-Addendum, vorausgesetzt, dies bleibt ein gültiger Übermittlungsmechanismus gemäß der UK GDPR; (c) alle anderen Standardvertragsklauseln oder Addendums für die Übermittlung personenbezogener Daten außerhalb des Vereinigten Königreichs, die gemäß der UK GDPR gültig sind; oder (d) ein anderer gültiger Übermittlungsmechanismus gemäß der Datenschutzgesetzgebung vorhanden ist. Zur Vermeidung von Zweifeln und vorbehaltlich des nachstehenden Absatzes 4 nimmt der Kunde zur Kenntnis und erklärt sich damit einverstanden, dass R&M nicht verpflichtet ist, Standardvertragsklauseln (einschließlich, aber nicht beschränkt auf die EU-Standardvertragsklauseln (Modul 2 - Vom Verantwortlichen zum Verarbeiter), oder andere Vereinbarungen mit Dienstleistern, einzugehen;

1.9 den Kunden unverzüglich zu benachrichtigen, wenn nach Ansicht von R&M eine Anweisung oder Weisung des Kunden gegen die Datenschutzgesetzgebung oder andere geltende Datenschutzvorschriften der Europäischen Union oder der Mitgliedstaaten verstößt; und

1.10 nach Wahl des Kunden alle Daten zu löschen oder an den Kunden zurückzugeben, wenn die Dienstleistungen für den Kunden eingestellt werden, und alle zu diesem Zeitpunkt vorhandenen Kopien zu löschen (es sei denn, R&M ist nach geltendem Recht zur Aufbewahrung verpflichtet).

2 Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, und stellt sicher, dass die Reisenden und Nutzer zur Kenntnis nehmen und sich damit einverstanden erklären, dass es für R&M notwendig ist, Daten an Dienstleister (unabhängig davon, ob sie im EWR ansässig sind oder nicht) zu übermitteln, um Dienstleistungen zu erbringen.

3 Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass R&M befugt ist, Unterauftragsverarbeiter in Bezug auf die Verarbeitung von Daten im Namen des Kunden für die Erbringung der Dienstleistungen gemäß diesem Vertrags einzusetzen. Eine Liste der von R&M eingesetzten Unterauftragsverarbeiter finden Sie hier. R&M bleibt verantwortlich und haftbar für alle Handlungen oder Unterlassungen seiner Unterauftragsverarbeiter. R&M stellt sicher, dass es einen schriftlichen Vertrag mit den Unterauftragsverarbeitern abgeschlossen hat, der Bedingungen für den Schutz von Daten enthält, die nicht weniger schützend sind als die in dieser Anlage aufgeführten Bedingungen.

4 Unbeschadet des obigen Absatzes 2 und ungeachtet anderer Bestimmungen in diesems Vertrag:

(a) erklärt sich der Kunde hiermit damit einverstanden, dass R&M Daten an einen Dienstleister (unabhängig davon, ob dieser im EWR oder im Vereinigten Königreich ansässig ist oder nicht) zum Zwecke der Erbringung der Dienstleistungen gemäß diesem Vertrag übermittelt; und

(b) stellt der Kunde sicher, dass die Reisenden und die Nutzer, soweit erforderlich, jeweils ihr Einverständnis dazu gegeben haben, dass R&M die Daten der Reisenden und der Nutzer zum Zweck der Erbringung der Dienstleistungen gemäß diesem Vertrag an die Dienstleister übermittelt.

5 In Anbetracht des obigen Absatzes 2 wird sich R&M in angemessener Weise bemühen, dem Kunden zu helfen, auf ein Versäumnis (sei es eine Handlung oder eine Unterlassung) eines Dienstleisters zu reagieren, Daten in Übereinstimmung mit angemessenen und branchenüblichen Methoden zu verarbeiten. Allerdingsübernimmt R&M jedoch ansonsten keine Haftung gegenüber dem Kunden, einem Mitglied der Gruppe des Kunden oder einem Reisenden oder Nutzer (sei es aus Vertrag, unerlaubter Handlung (einschließlich Fahrlässigkeit oder Verletzung gesetzlicher Pflichten), falscher Darstellung oder anderweitig), die sich aus oder in Verbindung mit der Verarbeitung, der Nutzung, dem Missbrauch, dem Verlust, der Beschädigung oder der Verfälschung von Daten durch einen Dienstleister oder der sonstigen Verletzung der Rechte einer Person in Bezug auf Daten ergibt.

6 Unbeschadet der obigen Absätze 2, 4 und 5 (einschließlich) dieser Anlage stellt der Kunde sicher, dass alle erforderlichen Rechtsgrundlagen vorhanden sind, gegebenfalls einschließlich der Einholung der Zustimmung, und stellt den Reisenden und Nutzern alle erforderlichen Informationen zur Verfügung, damit die Daten rechtmäßig und in Übereinstimmung mit den Datenschutzgesetzgebungenen an R&M übermittelt werden können.

7 Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass Anhang 1 dieser Anlage bestimmte Einzelheiten über die Verarbeitung von Daten durch R&M im Rahmen dieses Vertrags enthält.

8 Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass er die unverhältnismäßige Kosten und Ausgaben, die R&M durch die in den Absätzen 1.4 und 1.5 beschriebene Unterstützung entstanden sind, trägt und R&M diese erstattet.

9 In dem Maße, in dem: (a) das Vereinigte Königreich nicht Gegenstand eines Angemessenheitsbeschlusses der Europäischen Kommission ist; und (b) kein anderer gültiger Übermittlungsmechanismus nach der GDPR für die Übermittlung von Daten aus dem Europäischen Wirtschaftsraum in das Vereinigte Königreich zur Verfügung steht, schließen R&M und der Kunde die EU-Standardvertragsklauseln (Modul 2 - Vom Verantwortlichen zum Verarbeiter) in dem Umfang ab, der erforderlich ist, um die Verpflichtungen des Kunden als Verantwortlicher nach der GDPR in Bezug auf die Übermittlung von Daten an R&M im Vereinigten Königreich zu erfüllen.

10 Sofern nicht durch geltendes Recht untersagt, wird R&M (i) den Kunden unverzüglich über Anfragen, Anordnungen oder ähnliche Forderungen eines Gerichts, einer zuständigen Behörde, einer Strafverfolgungsbehörde oder einer anderen staatlichen Einrichtung ("Strafverfolgungsanfrage") in Bezug auf die Verarbeitung von Daten im Rahmen dieses Vertrags informieren und dem Kunden die Möglichkeit geben, gegen eine Strafverfolgungsanfrage Einspruch zu erheben; und (ii) alle angemessenen Maßnahmen ergreifen, um die Offenlegung von Daten, die von R&M im Rahmen dieses Vertrags als Reaktion auf eine Strafverfolgungsanfrage verarbeitet werden, ohne die ausdrückliche vorherige schriftliche Zustimmung des Kunden zu verhindern. Sollte es rechtlich nicht möglich sein, die Offenlegung von Daten, die von R&M im Rahmen dieses Vertrags verarbeitet werden, als Reaktion auf eine Strafverfolgungsanfragezu verhindern, ist der Kunde berechtigt, die Übermittlung dieser Daten auszusetzen und/oder den Vertrag durch schriftliche Mitteilung an R&M zu kündigen.

Anhang 1

Aktivitäten der Datenverarbeitung

Kategorien von Daten	Angaben zum Reisenden und/oder Buchenden - Anrede, Vorname, zweiter Vorname, Nachname, bekannter Name (falls abweichend), Geschlecht, Geburtsdatum, -ort und -land, Wohnsitzland, Staatsangehörigkeit, Familienstand; Aufenthaltsort des Reisenden - Reiseziele und Orte der Reise. Unternehmensinformationen - Firmenname, Abteilung, Kostenstelle, Kontonummer, Berufsbezeichnung, Mitarbeiternummer Wichtigste Kontaktinformationen - Adressen (Wohnsitz, Büros usw.), Telefonnummern, Faxnummern, Mobiltelefonnummern, E-Mail-Adresse Informationen zum Reisebucher/PA - Name, Telefonnummer, E-Mail-Adresse Zahlungsarten - Kartentyp, Kartennummer, Ablaufdatum, Nutzungspräferenzen, Debit-/Kreditkarte, persönlich/geschäftlich Dokumente - Reisepass - Land, in dem der Pass ausgestellt wurde, Passnummer, Vorname, zweiter Vorname, Nachname, Ausstellungsdatum, Ablaufdatum, biometrische Daten (J/N) Visum (inkl. ESTA, Redress, Schengen, Arbeitserlaubnis, Global Entry) - Visumbezirk, Ausstellungsland, Art des Visums, Dokumentennummer, Ausstellungsdatum und Ablaufdatum TSA - TSA-Nummer, Startdatum, Ablaufdatum Führerscheine - Land, Führerscheinnummer, Vorname, zweiter Vorname, Nachname, Startsdatum, Ablaufdatum, vorläufig (J/N), international (J/N) Ausweise - Land, Ausweisnummer, Vorname, zweiter Vorname, Nachname, Startdatum, Ablaufdatum Informationen zu Impfungen und Covid-19-Tests, die für Buchungen erforderlich sind Impfungen, Covid und Gesundheitsinformationen wie für Buchungen erforderlich Reisepräferenzen - Flug - Sitzplatztyp, Heimatflughafen, bevorzugter Online-Check-in, Mahlzeitentyp Auto - Kategorie, Stil, Getriebe, Kraftstoff/Klima, Satellitennavigation (J/N), Bahn - Sitzplatzzuweisung, Mahlzeitentyp Eurostar - Wagennummer, Sitzplatznummer, Sitzplatztyp, Sitzplatzzuweisung, Mahlzeitentyp Hotel - Raucher/Nichtraucher, bevorzugter Zimmertyp Alle Anforderungen an die Zugänglichkeit der Reise Mitgliedschaften - Treuekarten – Art der Dienstleistung, Anbieter, Mitgliedsnummer, Ablaufdatum, Status, Stufe Persönliche Hobbys/Interessen
Kategorien von betroffenen Personen	Mitarbeiter und Gäste des Kunden und andere Personen, für die der Kunde Reisen benötigt
Bearbeitung von Vorgängen	Bereitstellung von Reisen und reisebezogenen Dienstleistungen
Verwendungszwecke	Bereitstellung von Reisen und reisebezogenen Dienstleistungen
Dauer	Finanzen - Laufzeit des Vertrags + 10 Jahre Profile - Dauer des Vertrags, jährlich überprüft und auf Wunsch des Kunden gelöscht

Anhang 2

EU-Standardvertragsklauseln (Modul 2 -Vom Verantwortlichen zum Verarbeiter)

Anfangsdatum: Wie im Vertrag festgelegt

Exporteur *(der die eingeschränkte Übertragung sendet):*	Importeur (*der die eingeschränkte Übertragung erhält):*
Der Kunde, wie im Vertrag dargelegt	Reed & Mackay Deutschland GmbH, wie imVertragdargelegt
Wichtiger Ansprechpartner: Vollständiger Name: Berufsbezeichnung: Kontaktinformationen:	Wichtiger Ansprechpartner: Vollständiger Name: Berufsbezeichnung: Kontaktinformatione
Unterschrift:	Unterschrift:

1. Muster-Klauseln

Für die Zwecke dieses Vertragswerden die Musterklauseln wie folgt übernommen:

Modul in Betrieb:	Klausel 7 (Kopplungsklausel)	Klausel 9a (Vorabgenehmigung oder Allgemeingenehmigung)	Klausel 9a (Zeitspanne)	Klausel 11 (Option)	Klausel 17 (Option)	Klausel 18 (Option)
2	Integriert	Allgemeine Ermächtigung	15 Tage	Integriert	Das Recht eines EU-Mitgliedstaates, in dem der Datenexporteur niedergelassen ist	Die Republik Irland

Anwendbare Klauseln	Alle Klauseln des Moduls 2: Übertragung vom Verantwortlichen zum Verarbeiter, der Standardvertragsklauseln, die durch den Beschluss 2021/914 der Europäischen Kommission vom 4. Juni 2021 genehmigt wurden, sind in der vorliegenden Fassung anwendbar.

2. Appendix-Information

Wie im nachstehenden Appendix zu diesem Verzeichnis dargelegt.

Anhang 2 - Appendix 1

Beschreibung der Übertragung

Kategorien von betroffenen Personen, deren personenbezogene Daten übermittelt werden

Wie in Anhang 1 unter "Kategorien von betroffenen Personen" dargelegt.

Kategorien der übermittelten personenbezogenen Daten

Wie in Anhang 1 unter " Kategorien von Daten" dargelegt.

Übermittlung sensibler Daten (falls zutreffend) und Anwendung von Beschränkungen oder Garantien, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strikte Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnung des Zugangs zu den Daten, Beschränkungen für die Weiterübermittlung oder zusätzliche Sicherheitsmaßnahmen.

R&M verarbeitet nicht routinemäßig Daten der besonderen Kategorie. Im Zusammenhang mit der erbrachten Reiseleistung können sensible Daten abgeleitet werden, z. B. wenn Hilfe benötigt wird (was auf einen Gesundheitszustand hindeuten kann), Informationen zu Impfungen und/oder Tests (wie für Buchungen erforderlich, was auf den Gesundheitszustand hindeuten kann) und Essensvorlieben (woraus auf die Religion geschlossen werden könnte). R&M wendet für alle personenbezogenen Daten das gleiche hohe Sicherheitsniveau an.

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden).

Die Übermittlung erfolgt fortlaufend zum Zwecke der Erbringung von Reise- und reisebezogenen Dienstleistungen.

Art der Verarbeitung

Wie in Anhang 1 unter " Bearbeitung von Vorgängen" dargelegt.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Wie in Anhang 1 unter "Verwendungszwecke" dargelegt

Der Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder, falls dies nicht möglich ist, die Kriterien, nach denen dieser Zeitraum festgelegt wird

Wie in Anhang 1 unter "Dauer" dargelegt.

Bei Übermittlungen an (Unter-)Verarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben

https://clientportal.reedmac.com/knowledgehub/SubProcessors

Nennen Sie die zuständige(n) Aufsichtsbehörde(n) gemäß Klausel 13

Irish Data Protection Authority (*Irische Datenschutzbehörde*)

Anhang 2 - Appendix 2

Technische und organisatorische Maßnahmen einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Daten

Beschreibung der von dem/den Datenimporteur(en) getroffenen technischen und organisatorischen Maßnahmen (einschließlich etwaiger einschlägiger Zertifizierungen) zur Gewährleistung eines angemessenen Sicherheitsniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

Version 2.5 - Juli 2024 (kann von R&M aktualisiert werden)

DEFINITION

"Personal" bezeichnet die Mitarbeiter, Auftragnehmer oder Berater von Reed & Mackay, die an der Erbringung der Dienstleistungen von Reed & Mackay für seine Kunden beteiligt sind.

"Daten" bezeichnet die Daten von Reed & Mackay, einschließlich aller Daten von Kunden, die Reed & Mackay vom Kunden (Verantwortlicher) in Übereinstimmung mit Datenverarbeitungsverträgen, Standardvertragsklauseln und/oder Verträgen zwischen dem Kunden und Reed & Mackay zur Verfügung gestellt werden.

EINFÜHRUNG

Das Führungsteam (*Executive Team*) von Reed & Mackay ist sich der Bedeutung der Informationssicherheit bewusst, und die Aufrechterhaltung der höchsten Standards für Vertraulichkeit, Integrität und Verfügbarkeit von internen, Kunden- und Lieferantendaten ist von grundlegender Bedeutung für unsere Vision, "das am meisten geschätzte, empfohlene und unternehmerisch denkende Reise-, Beratungs- und Veranstaltungsunternehmen der Welt zu sein".

Wie in diesem Dokument beschrieben, unterhält Reed & Mackay eine Reihe von technischen und organisatorischen Sicherheitsmaßnahmen, die mit den besten Praktiken und Standards der Branche übereinstimmen, sowie Zertifizierungen, die wir aufrechterhalten, um die Risiken für Daten, Informationswerte, Dienstleistungen, Leistung, Kundenvertrauen oder andere Bereiche des Unternehmens, die sich aus einem Versagen der Informationssicherheit ergeben könnten, zu verringern.

1. 1. ZERTIFIZIERUNGEN

1.1. Reed & Mackay verfügt über die Zertifizierungen nach ISO/IEC 27001, dem internationalen Standard für Informationssicherheitsmanagement (*international standard for Information Security Management*), ISO 22301 - Unternehmenskontinuitätmanagement (*Business Continuity Management*), ISO 9001 - Qualitätsmanagement (*Quality Management*) und ISO 14001 – Umweltmanagement (*Environmental Management*). Reed & Mackay ist auch nach PCI-DSS - The Payment Card Industry - Data Security Standard - zertifiziert, der auch eine Voraussetzung für die IATA-Lizenzierung ist und daher von Reed & Mackay sehr ernst genommen wird.

1.2. Die Zertifizierungen werden durch ein externes und ein internes Auditprogramm aufrechterhalten, das regelmäßige interne und jährliche externe Audits sowie kontinuierliche Verbesserungsmaßnahmen umfasst.

2. INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM

2.1. Die Informationssicherheitsrichtlinien von Reed & Mackay geben eine klare Richtung für die Informationssicherheit vor und zeigen die Unterstützung und das Engagement für das Management der Informationssicherheit im gesamten Unternehmen.

2.2. Die Informationssicherheit wird durch eine Reihe strenger Kontrollen verwaltet, darunter Richtlinien, Prozesse, Verfahren, Software- und Hardwarefunktionen, die das Informationssicherheitsmanagementsystem (ISMS) von Reed & Mackay bilden. Diese Kontrollen werden überwacht, überprüft und gegebenenfalls verbessert, um sicherzustellen, dass die spezifischen Sicherheits- und Geschäftsziele erreicht werden.

2.3. Jedes Personal erhält bei ihrem Eintritt in das Unternehmen ein umfassendes und obligatorisches Einführungs- und Schulungsprogramm sowie eine jährliche Auffrischung zur Einhaltung der Vorschriften, einschließlich Informationssicherheit und Datenschutz.

2.4. Die letztendliche Verantwortung für die Informationssicherheit liegt beim Chief Information Officer, aber diese Verantwortung wird durch den designierten Direktor für Sicherheit & Vertrauen (*Director of Security & Trust*) wahrgenommen, der die Hauptverantwortung für die Informationssicherheit, das Informationssicherheitsrisiko, die Cybersicherheit und das Management von Sicherheitsvorfällen innerhalb von Reed & Mackay trägt und als zentrale Anlaufstelle für die Informationssicherheit sowohl für Personal als auch für externe Organisationen fungiert.

2.5. Die Abteilungsleiter (*Heads of Departments*) sind für die Durchsetzung der Informationssicherheitsrichtlinien in ihren Geschäftsbereichen und für die Einhaltung dieser Richtlinien durch ihr Personal verantwortlich. Jedes Personal ist für die Informationssicherheit verantwortlich; sie müssen sicherstellen, dass sie die einschlägigen Unternehmensrichtlinien, -prozesse und -verfahren befolgen, sich der Bedeutung der Informationssicherheit und der potenziellen Risiken bewusst sind und alle Vorfälle, Ereignisse oder potenziellen Schwachstellen melden.

3. SICHERHEIT DER PERSONALABLEITUNG (*HUMAN RESOURCES*)

3.1. Reed & Mackay arbeitet eng mit unseren Personalvermittlern zusammen, um sicherzustellen, dass die Anforderungen an die Einstellungsvoraussetzungen in unserem Namen erfüllt werden.

3.2. Reed & Mackay beauftragt ein externes Unternehmen mit der Durchführung von Hintergrunduntersuchungen (*Background Screening*) in Übereinstimmung mit dem *Baseline Personnel Security Standard (BPSS)* der britischen Regierung für jedes Personal, unabhängig von ihrer Funktion, vorbehaltlich der Einschränkungen in Übereinstimmung mit der lokalen Gesetzgebung.

3.3. In den Verträgen mit Personal sind Vertraulichkeitsklauseln enthalten, die einen angemessenen Schutz der Vertraulichkeit von Reed & Mackay-Daten gewährleisten.

3.4. Es gibt ein Disziplinarverfahren für die Nichteinhaltung von Sicherheitsrichtlinien und -anforderungen.

3.5. Bei Beendigung des Beschäftigungsverhältnisses wird dem Personal am letzten Arbeitstag der Zugang entzogen, und alle Ausrüstungsgegenstände und das geistige Eigentum werden vom Ausscheidenden zurückgegeben.

4. VERMÖGENSVERWALTUNG AND DATENSICHERHEIT

4.1. Die mit Informationen und informationsverarbeitenden Einrichtungen verbundenen Vermögenswerte werden identifiziert und ein Inventar der Vermögenswerte wird geführt.

4.2. Informationen und Daten werden gemäß einer vom Management genehmigten Richtlinie zur Klassifizierung von Informationen, Vermögen und Datenmanagement klassifiziert und verwaltet.

4.3. Nur vertrauenswürdige Geräte haben Zugang zu den Ressourcen des Unternehmensnetzwerks von Reed & Mackay. Dazu gehören Computer, die mit der Reed & Mackay-Domäne verbunden sind, und mobile Geräte, die bei der Lösung für das Management mobiler Geräte (*Mobile Device Management Solution*) von Reed & Mackay angemeldet wurden und den Sicherheitsrichtlinien entsprechen.

4.4. Die Anforderungen an die Sicherheitskontrollen für persönliche und von Reed & Mackay ausgegebene mobile Geräte sind in der Richtlinie für mobile und persönliche Geräte (*Mobile and Personal Device policy*) festgelegt. Zu den Kontrollen gehören unter anderem Verschlüsselung, Fernlöschung und deaktivierte USB-Anschlüsse.

4.5. Alle Endpunkte sind verschlüsselt. USB-Anschlüsse und die Verwendung von Wechselmedien sind eingeschränkt.

4.6. Technische DLP-Maßnahmen sowie eine Richtlinie für einen geräumten Schreibtisch und Bildschirm "*Clear Desk & Clear Screen policy*" sollen das Risiko von Datenlecks und der versehentlichen Offenlegung von Reed & Mackay-Daten verringern.

4.7. Es gibt eine Richtlinie für die Datenaufbewahrung (*Data Retention Policy*) und einen Zeitplan für die Datenaufbewahrung (*Data Retention Schedule*), um die Anforderungen an die Datenaufbewahrung in Übereinstimmung mit der Datenschutz-Grundverordnung und dem GDPR festzulegen sowie die Anforderungen an die sichere Datenentsorgung von sensiblen Daten auf physischen oder elektronischen Medien gemäß anerkannten Sicherheitsstandards / Best Practices der IT-Branche (z. B. CESG oder vom Verteidigungsministerium (*DOD*) genehmigte Standards).

4.8. Datenträger, die Informationen enthalten, werden gemäß den von der WEEE (Waste Electrical and Electronic Equipment) und der CESG (Communications Electronics Security Group) genehmigten Standards für die Datenvernichtung auf sichere Art und Weise vernichtet. Die Abteilung für Technische Dienste (*Tech Services Department*) führt Aufzeichnungen.

4.9. Die sichere Vernichtung von Dokumenten erfolgt entweder durch den Einsatz von Aktenvernichtern mit Querschnitt oder durch zugelassene Dritte, die Dienstleistungen gemäß der Norm BS EN 15713 für Sicherheitsvernichtung und mindestens der Sicherheitsstufe DIN P-3 für vertrauliche Dokumente anbieten.

5. ZUGANGSKONTROLLE

5.1. Es gibt ein rollenbasiertes Zugangskontrollmodell (R*ole Based Access Control*), bei dem den einzelnen Personen Rollen zugewiesen werden, die auf der Grundlage ihrer Aufgaben und der Notwendigkeit, etwas zu wissen, beruhen.

5.2. Die Grundsätze der Aufgabentrennung und der geringstmöglichen Privilegierung (*Separation of Duties and Least privilege Principles*) werden befolgt, und privilegierter Zugang wird nach dokumentierter Genehmigung durch die Geschäftsleitung gewährt.

5.3. Privilegierte IT-Verwaltungsrechte werden über eine separate Benutzerkennung (*User ID*) (erhöhtes Konto) für die normale Benutzerkennung des Benutzers bereitgestellt.

5.4. Wir überwachen alle Ereignisse im Zusammenhang mit der Anmeldung an Servern und Workstations mit administrativen Konten sowie Änderungen an Berechtigungsgruppen.

5.5. Die Überprüfung der Zugriffsrechte (*Access Rights Reviews*) wird in regelmäßigen Abständen durchgeführt, wobei die Häufigkeit von der Kritikalität des Informationsguts abhängt und zwischen vierteljährlich und jährlich variiert.

5.6. Die Passwortrichtlinie (*Password Policy*) von Reed & Mackay ist wie folgt definiert: Passwörter müssen mindestens 12 Zeichen enthalten, mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl oder ein Sonderzeichen. Passwörter müssen internationale Zeichen (nicht-ASCII) vermeiden, dürfen keine Wörter aus dem Wörterbuch oder Informationen über den Benutzer enthalten (wie die Benutzer-ID, Namen von Familienmitgliedern, Geburtsdatum usw.), müssen mindestens einmal alle 90 Tage geändert werden und dürfen nicht mit den 24 zuvor verwendeten Passwörtern identisch sein.

5.7. Benutzerkonten werden nach 5 ungültigen Anmeldeversuchen gesperrt und bleiben so lange gesperrt, bis ein Administrator oder der Benutzer sie entsperrt (letzteres erfolgt über Self-Service und Multifaktor-Authentifizierung).

5.8. Die Multifaktor-Authentifizierung wird für alle Benutzer- und Administratorkonten von Reed & Mackay durchgesetzt.

6. KRYPTOGRAPHIE

6.1. Wie in der Kryptografierichtlinie (*Cryptography Policy*) von Reed & Mackay definiert, werden kryptografische Kontrollen eingesetzt, um sensible Daten sowohl während der Übertragung als auch im Ruhezustand zu schützen.

6.2. Die Verschlüsselung auf mobilen Geräten wird über Microsoft Intune Endpoint Manager-Richtlinien durchgesetzt.

6.3. Die Verschlüsselung der PII-Datenbank erfolgt über Thales CipherTrust (AES 256-Bit-Verschlüsselung, Daten-Tokenisierung und Verschlüsselungsdienste).

6.4. Die Datenbank wird mit der transparenten Datenverschlüsselung (*Transparent Data Encryption*) (TDE) AES-256 verschlüsselt.

6.5. Der gesamte Verkehr von/zu unseren öffentlich zugänglichen Anwendungen (Webseiten + Mobile App) verwendet HTTPS-Zertifikate, die von der GlobalSign-Zertifizierungsstelle (*GlobalSign Certificate Authority*) ausgestellt und mit TLS 1.2 oder höher verschlüsselt sind.

6.6. Alle Backups sind verschlüsselt.

7. BETRIEBSSICHERHEIT

7.1. Änderungen an Produktionsumgebungen werden im Einklang mit der IT-Änderungsrichtlinie (*IT Change Management Policy*) von Reed & Mackay kontrolliert.

7.2. Malware-Erkennung, -Prävention und -Wiederherstellungskontrollen zum Schutz vor Malware werden durch eine Anti-Malware-Lösung der nächsten Generation bereitgestellt.

7.3. Es gibt ein umfassendes Patch-Management-Verfahren. Patches und Sicherheitsupdates werden monatlich eingespielt, oder häufiger, wenn ein erhebliches Sicherheitsrisiko festgestellt wird. Die Patch-Verwaltung unterliegt der Änderungskontrolle und der IT-Änderungsrichtlinie (*IT Change Management Policy*).

7.4. Es gibt ein technisches Programm zum Management von Schwachstellen, das auch ein laufendes Programm zur Behebung von Schwachstellen umfasst. Schwachstellen werden durch interne und externe Infrastruktur-Scans, vierteljährliche PCI-DSS ASV-Scans und Penetrationstests ermittelt.

7.5. Es gibt ein umfassendes jährliches Penetrationstestprogramm, das von CREST-akkreditierten unabhängigen Penetrationstestern durchgeführt wird. Dies betrifft die gesamte kritische Infrastruktur von R&M.

8. PROTOKOLLIERUNG, ÜBERWACHUNG & VERWALTUNG VON SICHERHEITSVORFÄLLEN

8.1. Ereignisprotokolle, die Benutzeraktivitäten, Ausnahmen, Fehler und Informationssicherheitsereignisse aufzeichnen, werden erstellt, aufbewahrt, vor Manipulationen geschützt und regelmäßig überprüft.

8.2. Über einen vertrauenswürdigen Drittanbieter von verwalteten Sicherheitsdiensten (*third-party Managed Security Services Provider*) wird rund um die Uhr ein Sicherheitsoperationszentrum (*Security Operations Centre*) (SOC) betrieben, das Überwachung, Protokollerfassung und -analyse, Sicherheitsinformations- und Ereignisverwaltung (SIEM), Reaktion auf Sicherheitsvorfälle und Schadensbegrenzung sowie forensische Analysefunktionen umfasst, um die Ursachen von Sicherheitsvorfällen zu verstehen und Methoden zur Verringerung oder Beseitigung potenzieller Angriffsflächen zu finden.

8.3. Beobachtete oder vermutete Sicherheitsvorfälle werden zentral gemeldet, automatisch protokolliert und vom Sicherheitsvorfall-Reaktionsteam (*Security Incident Response Team*) in Übereinstimmung mit dem Plan zur Reaktion auf Informationssicherheitsvorfälle (*Information Security Incident Response Plan*) und dem Prozess für das Management von Datenverletzungen (*Data Breach Management Process*) (falls zutreffend) weiterverfolgt.

9. CLOUD SICHERHEIT

9.1. Die Reisemanagement-Plattform (*Travel Management Platform*) und die Server-Infrastruktur von Reed & Mackay werden im Rechenzentrum von Microsoft Azure in Süd-Großbritannien gehostet.

9.2. MS Azure ist so konfiguriert, dass Informationen im Ruhezustand unabhängig vom Speichermedium verschlüsselt werden, sei es eine verwaltete Festplatte, die an eine virtuelle Maschine angeschlossen ist, ein Speicherkonto, das Telemetriedaten oder Anwendungsquellcode enthält, oder ein Plattformdatenbankdienst wie Microsoft SQL.

9.3. Es gibt eine vom Management genehmigte Cloud-Sicherheitsrichtlinie (*Cloud Security Policy*), in der die Anforderungen an die Cloud-Sicherheit festgelegt sind.

9.4. Eine Lösung für die Verwaltung der Cloud-Sicherheitslage (*Cloud Security Posture Management solution*) überwacht und verwaltet die Verwaltung der Microsoft Azure-basierten Ressourcen und Dienste von Reed & Mackay, einschließlich der Visualisierung und Bewertung der Sicherheitslage, der Erkennung von Fehlkonfigurationen und der Durchsetzung bewährter Sicherheitspraktiken (*Best Practices*) und Einhaltungsrahmen (*Compliance-Frameworks*).

9.5. Microsoft Netzwerksicherheitsgruppen (*Network Security Groups*) und virtuelle Firewall-Geräte (*Firewall-Appliances*) der nächsten Generation von Checkpoint schützen unsere Umgebung am Perimeter mit aktiviertem Eindringungsschutz (*Intrusion Prevention*).

10. PHYSISCHE SICHERHEIT

10.1. In Übereinstimmung mit unserer Sicherheitsrichtlinie für physische und ökologische Sicherheit sind angemessene physische und ökologische Sicherheitsmaßnahmen vorhanden, um unbefugten physischen Zugang, Beschädigung und Störung von Reed & Mackay-Daten, Räumlichkeiten und Verarbeitungseinrichtungen zu verhindern. Die folgenden Kontrollen sind vorhanden:

10.1.1. Hauptsitz: Die Rezeption des Gebäudes ist rund um die Uhr besetzt, die Rezeption von Reed & Mackay ist während der Bürozeiten besetzt. CCTV an allen Gebäudezugängen, die die meisten allgemeinen Bereiche sowie die Bereiche, in denen man das Gebäude betritt und verlässt, überwachen. Der Zugang zum IT-Kommunikationsraum (*IT Comms room*) erfolgt über ein Magnetkartensystem und ein Tastatureingabesystem. Der Zugang ist auf befugte Personen mit einem geschäftlichen Bedarf beschränkt.

10.1.2. Regionalbüros: In den Regionalbüros werden mit einigen Ausnahmen die gleichen Kontrollen durchgeführt wie im Hauptsitz. Unsere kleineren Büros verfügen nicht über einen rund um die Uhr besetzten Empfang oder ein Zugangskartensystem, jedoch sind kompensierende Kontrollen in Übereinstimmung mit unserer physischen und

ökologischen Sicherheits-Rechtlinie (*Physical and Environmental Security Policy*) vorgesehen, um sicherzustellen, dass die physische Sicherheit in diesen Büros angemessen ist.

10.2. Besucher erhalten nur zu bestimmten und genehmigten Zwecken Zutritt und werden in den Büros von Reed & Mackay stets beaufsichtigt/begleitet. Besucherprotokolle werden für jeden physischen Zugang zu den Büros, Serverräumen und Datenzentren von Reed & Mackay geführt, in denen sich die IT-Ausrüstung und die Datenbestände von Reed & Mackay befinden.

11. KOMMUNICATION & NETZSICHERHEIT

11.1. Die Netze werden durch geeignete Sicherheitskontrollen wie Netzsegmentierung, Netzzugangsverwaltung, Firewalls, Konfigurationsstandards sowie Protokollierung und Überwachung verwaltet.

11.2. Es gibt Verfahren und Kontrollen für die Informationsübertragung, um die Übertragung von Daten über alle Arten von Kommunikationseinrichtungen zu schützen.

11.3. Unser empfohlenes Datenübertragungsprotokoll für den regelmäßigen Datenaustausch (z. B. Datendateien, HR-Feeds) besteht darin, eine SFTP-Verbindung zwischen den Organisationen herzustellen - welche Partei die Daten schiebt/zieht, bleibt den Parteien überlassen.

12. SOFTWARE-ENTWICKLUNG

12.1. Die interne Softwareentwicklung folgt der Agile/Sprint-Lebenszyklusmethodik (*Agile/Sprint life-cycle methodology*) und den Bewährte OWASP-Praktiken (*OWASP Best Practices*).

12.2. Es gibt eine SDLC (Software-Entwicklungslebenszyklus) Richtlinie (*Software Development Lifecycle Policy*), die Anforderungsanalyse und -spezifikationen, Sicherheit durch Design, sichere technische Grundsätze, sichere Entwicklungsumgebung, Anwendungsunterstützung, Qualitätssicherung, Tests, Implementierung, Schulung und Überprüfung nach der Implementierung umfasst.

12.3. Single-Sign-On-Integration ist in unseren kundenorientierten Anwendungen verfügbar. SAML 2.0-basierte Lösungen wie Azure AD, Ping Identity, Duo und Okta werden unterstützt, andere Optionen von Drittanbietern können ebenfalls unterstützt werden, erfordern aber möglicherweise Entwicklung und Tests.

12.4. Entwicklungs-, Test- und Produktionssysteme sind voneinander getrennt. Anonymisierte Daten werden für Testzwecke in Nicht-Produktionsumgebungen (*non-production environments*) verwendet.

12.5. Die Kundendaten werden durch eindeutige Identifikatoren getrennt, die zum Zeitpunkt der Einrichtung des Kontos zugewiesen werden. Die Trennung wird durch die Verwendung eindeutiger Identifikatoren gewährleistet, z. B. Unternehmens-IDs, Reisenden-IDs und Konto-IDs.

13. BEZIEHUNGEN MIT AUFTRAGNEHMERN

13.1. Neue Direktauftragnehmer (einschließlich Daten-Subverarbeiter) werden einer Due-Diligence-Prüfung unterzogen, die die Bereiche Informationssicherheit, Datenschutz, Geschäftskontinuität, Unternehmensführung und Qualität, Gesundheit und Sicherheit, Umwelt, Chancengleichheit, Vielfalt, Bekämpfung von Bestechung und Korruption, moderne Sklaverei und Kinderarbeit, ethische Geschäftspraktiken / soziale Verantwortung des Unternehmens sowie gegebenenfalls eine Bonitätsprüfung, eine Überprüfung der Richtlinien, Zertifizierungen, unabhängige Prüfberichte, unabhängige Penetrationstests (inkl. Folgemaßnahmen) usw. umfasst.

13.2. Die Auftragnehmer unterliegen in ihren Verträgen Vertraulichkeits- und Audit-Klauseln.

13.3. Auftragnehmer sind verpflichtet, die Betriebsgrundsätze für Auftragnehmer (*Supplier Operating principles*) von Reed & Mackay einzuhalten, und Auftragnehmer von Produkten/Dienstleistungen, die mit R&M-Informationssystemen interagieren oder personenbezogene Daten verarbeiten, müssen vertraglich unseren Anforderungen an die Informationssicherheit von Auftragnehmern (*Supplier Information Security Requirements*) zustimmen.

13.4. Die Auftragnehmer werden in regelmäßigen Abständen überprüft. Art, Umfang und Häufigkeit dieser Überprüfung hängen von mehreren Faktoren ab, darunter das gelieferte Produkt/die Dienstleistung und die Kritikalität des Auftragnehmers.

13.5. Die Ausfallsicherheit und Wiederherstellungsfähigkeiten kritischer Auftragnehmer werden jährlich im Rahmen unserer Analyse der Geschäftsauswirkungen (*Business Impact Analysis*) (BIA) unserer BC-Wiederherstellungsfähigkeiten formell überprüft.

14. GESCHÄFTSKONTINUITÄT AND NOTFALLWIEDERHERSTELLUNG

14.1. Im Einklang mit unserer ISO 22301-Zertifizierung werden die Unternehmenskontinuitätpläne (*Business Continuity Plans*), einschließlich des Krisenmanagementplans (*Crisis Management Plan*) von Reed & Mackay, jährlich oder bei Bedarf auch häufiger (z. B. bei wesentlichen Änderungen) formell überprüft.

14.2. Es gibt ein fortlaufendes Übungs- und Testprogramm zur Aufrechterhaltung des Unternehmens (*Business Continuity*), das aus Szenarioübungen am Schreibtisch und physischen Wiederherstellungstests vor Ort besteht.

14.3. Jährlich wird eine Analyse der Auswirkungen auf das Unternehmen (*Business Impact Analysis*) durchgeführt, um das Ausmaß der Unterbrechung der wichtigsten Aktivitäten zu bestimmen, das Mindestmaß dieser Aktivitäten, das für das Unternehmen erforderlich ist, und die Ressourcen und Abhängigkeiten, die für die Wiederaufnahme der Aktivitäten erforderlich sind.

14.4. Die Reisemanagement-Plattform (*Travel Management Platform*) von Reed & Mackay wird in Microsoft Azure gehostet, was ein hohes Maß an Redundanz und Ausfallsicherheit bietet.

14.5. Ein Online-Backup-Service eines Drittanbieters, der sicherstellt, dass wichtige Informationen, die in virtuellen Maschinen und Speicherkonten enthalten sind, sicher und unabhängig von der Azure-Umgebung gespeichert werden und im Falle eines versehentlichen Verlusts oder einer Beschädigung zur Wiederherstellung zur Verfügung stehen.

14.6. Unsere firmeneigene Datenbank, einschließlich aller Buchhaltungs-, Kunden- und Berichtsdaten, unterliegt einer täglichen Vollsicherung und inkrementellen Sicherungen im Laufe des Tages. Das RPO liegt bei 1 Stunde und das RTO bei 3 Stunden. Server werden täglich auf einer "inkrementellen für immer"-Basis *("incremental forever" basis*) gesichert. Das RPO liegt bei 1 Tag, das RTO bei 4 Stunden. Unser Gesamt-RTO beträgt 4 Stunden.

14.7. Die Backups werden verschlüsselt und regelmäßig getestet.

15. INFORMATIONSSICHERHEITSRISIKO

15.1. Risikobasiertes Denken und Bewusstsein ist in das Managementsystem von Reed & Mackay und die ihm zugrunde liegenden Prozesse integriert.

15.2. Das Risikomanagementprogramm für die Informationssicherheit (*Information Security Risk Management Program*) ist Teil des Rahmens für das Risikomanagement des Unternehmens (*Corporate Risk Management Framework*) und umfasst die Identifizierung und Bewertung von Informationssicherheitsrisiken, die sich sowohl aus verschiedenen regelmäßigen Aktivitäten als auch aus geplanten und ungeplanten Veränderungen ergeben. Identifizierte Risiken werden nach Prioritäten geordnet, behandelt/akzeptiert und rechtzeitig genehmigt.

15.3. Die Aktivitäten im Rahmen des Informationssicherheitsmanagements (*Information Security Management program*)von Reed & Mackay werden auf der Grundlage der ermittelten Risiken und ihrer Auswirkungen auf die für die Kunden erbrachten Dienstleistungen nach Prioritäten geordnet.

Anhang 3

UK Addendum

Tabelle 1: Parteien

Anfangsdatum		
Die Parteien	**Exporteur (der die eingeschränkte Übertragung sendet)**	**Importeur (der die eingeschränkte Übertragung erhält)**
Angaben zu den Parteien	Gemäß der EU-Standardvertragsklauseln oben	Gemäß der EU-Standardvertragsklauseln oben
Wichtiger Ansprechpartner	GGemäß der EU-Standardvertragsklauseln oben	Gemäß der EU-Standardvertragsklauseln oben
Unterschrift		

Tabelle 2: Ausgewählte SCCs, Module und ausgewählte Klauseln

Addendum EU-Standardvertragsklauseln	☒ Die Version der genehmigten EU-Standardvertragsklauseln, der dieser Nachtrag beigefügt sind, werden im Folgenden einschließlich der Anhangsinformationen näher erläutert: Datum:

Tabelle 3: Anhangsinformationen

"**Anhangsinformationen**" sind die Informationen, die für die ausgewählten Module gemäß dem Anhang der genehmigten EU-Standardvertragsklauseln (mit Ausnahme der Parteien) bereitgestellt werden müssen und die für dieses Addendum in enthalten sind:

Anhang 1A: Liste der Parteien: Appendix der genehmigten EU-Standardvertragsklauseln, wie in der Anlage aufgeführt.
Anhang 1B: Beschreibung der Übertragung: Appendix der genehmigten EU-Standardvertragsklauseln, wie in der Anlage aufgeführt.
Anhang II: Technische und organisatorische Maßnahmen einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Daten: Appendix der genehmigten EU-Standardvertragsklauseln, wie in der Anlage aufgeführt.
Anhang III: Liste der Unter-Verarbeiter (nur Module 2 und 3): Appendix der genehmigten EU-Standardvertragsklauseln, wie in dieser Anlage aufgeführt.

Tabelle 4: Beendigung dieses Addendums bei Änderungen des genehmigten Addendums

Beendigung dieses Addendums bei Änderungen des genehmigten Addendums	Die Parteien können dieses Addendum nach Maßgabe von Abschnitt 19 beenden: ☐ Importeur ☒ Exporteur ☐ keine Partei

Obligatorische Klauseln	Teil 2: Obligatorische Klauseln des genehmigten Addendums, wobei es sich um die Vorlage Addendum B.1.0 handelt, die vom ICO herausgegeben und dem Parlament gemäß s119A des Data Protection Act 2018 am 2. Februar 2022 vorgelegt wurde, in der gemäß Abschnitt 18 dieser obligatorischen Klauseln überarbeiteten Fassung.