Vereinbarung über die Datenverarbeitung

DEN ZWECK & DIE REIHENFOLGE DES VORRANGS

Diese Datenverarbeitungsvereinbarung (die "**DPA**") gilt zusammen mit ihren Anhängen und allen Dokumenten, auf die ausdrücklich Bezug genommen wird (die "Vereinbarung"), als Teil der Dienstleistungsvereinbarung zwischen Iron Mountain und dem Kunden (die "**Vereinbarung**"). Die Bestimmungen und Bedingungen des Abkommens gelten für die Rechte und Pflichten der Parteien im Rahmen dieser DPA.

Sollte eine der Bestimmungen dieser DPA im Widerspruch zu den Bestimmungen des Abkommens stehen, so gelten die Bestimmungen dieser DPA für den Gegenstand dieser DPA. Diese DPA ersetzt alle früheren Datenverarbeitungsverträge, Datenschutz- oder Geheimhaltungsklauseln oder sonstigen Vereinbarungen zwischen den Parteien in Bezug auf die im Rahmen der Vereinbarung erbrachten Dienstleistungen und macht sie überflüssig.

ALLGEMEINE BEDINGUNGEN

1. DEFINITIONEN

Sofern nicht anders angegeben, haben alle in Großbuchstaben geschriebenen Begriffe die gleiche Bedeutung wie im Abkommen definiert.

"**Auftragsverarbeiter**" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

"**Betroffene Person**" ist eine identifizierte oder identifizierbare natürliche Person;

"**Dienstleistungen**" sind alle Dienstleistungen, die Iron Mountain oder seine verbundenen Unternehmen dem Kunden oder seinen verbundenen Unternehmen im Rahmen des Vertrags erbringen;

Der Begriff "**für die Verarbeitung Verantwortlicher**" bezieht sich auf eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die unabhängig oder in Zusammenarbeit mit anderen über die Gründe und Methoden der Verarbeitung personenbezogener Daten entscheidet;

Der Begriff "**personenbezogene Daten**" bezieht sich auf alle Informationen über eine betroffene Person;

"**Personenbezogene Daten des Kunden**" bezieht sich auf personenbezogene Daten, die im Rahmen der Dienste verarbeitet werden und die dem Kunden oder seinen verbundenen Unternehmen gehören oder von diesen gesammelt werden;

"Rechtsvorschriften über den Datenschutz" bezeichnet alle anwendbaren Gesetze und Vorschriften in Bezug auf die Verarbeitung personenbezogener Daten, die in den jeweiligen Rechtsordnungen bestehen können, einschließlich, aber nicht beschränkt auf die EU-DSGVO (Verordnung (EU) 2016/679), die britische GDPR (die GDPR als Teil des nationalen Rechts des Vereinigten Königreichs gemäß Abschnitt 3 des European Union (Withdrawal) Act 2018 und in der durch die Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (in der geänderten Fassung)), Data Protection Act 2018, FADP (das Schweizer Bundesgesetz über den Datenschutz), U.S. Staatliche Datenschutzgesetze, LGPD (brasilianisches allgemeines Datenschutzgesetz), PIPL (Gesetz der Volksrepublik China zum Schutz personenbezogener Daten) und alle Gesetze und/oder Verordnungen, die diese umsetzen oder durchsetzen, sowie alle Änderungen, Ersetzungen, Wiederinkraftsetzungen oder Konsolidierungen, gegebenenfalls einschließlich der von Aufsichtsbehörden herausgegebenen Leitlinien und Verfahrensregeln;

Iron Mountain, seine Mitarbeiter oder seine Subunternehmer verarbeiten personenbezogene Kundendaten im Rahmen der Erbringung der Dienstleistungen, und der Begriff "**Sicherheitsverletzung**" bezieht sich auf jede versehentliche oder unrechtmäßige Beschädigung, Zerstörung, jeden Verlust, jede Änderung oder unbefugte Offenlegung dieser Daten bzw. jeden unbefugten Zugriff auf diese Daten;

“**U.S.** Der Ausdruck **"staatliche Datenschutzgesetze"** bezieht sich auf alle Bundes- und einzelstaatlichen Gesetze zum Schutz der Privatsphäre und zum Datenschutz, die auf die Verarbeitung personenbezogener Daten im Rahmen der Vereinbarung anwendbar sind, einschließlich, aber nicht beschränkt auf die von Zeit zu Zeit geänderten, ersetzten oder ersetzten Gesetze: (1) das kalifornische Gesetz zum Schutz der Privatsphäre der Verbraucher, geändert durch das kalifornische Zusätzlich zum Privacy Rights Act und den dazugehörigen Durchführungsverordnungen (zusammen der "**CCPA**"); (2) dem Colorado Privacy Act ("**CPA**"), (3) dem Virginia Consumer Data Protection Act ("**CDPA**"); (4) dem Utah Consumer Privacy Act ("**UCPA**"); und (5) dem Connecticut Data Privacy Act ("**CTDPA**").

"**Verarbeitung**" ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder einer Reihe personenbezogener Daten, einschließlich des Erhebens, Aufzeichnens, Ordnens, Strukturierens, Speicherns, Anpassens oder Veränderns, Abrufens, Abfragens, Nutzens, Offenlegens durch Übermittlung, Verbreitung oder andere Formen der Bereitstellung, Abgleichung oder Kombinierens, Einschränkens, Löschens oder Vernichtens;

2. UMFANG UND EINZELHEITEN DER DATEN VERARBEITUNG

2.1 Diese DPA gilt für die personenbezogenen Daten des Kunden, die von Iron Mountain als Auftragsverarbeiter im Namen des Kunden im Rahmen der Erbringung der vertragsgemäßen Dienstleistungen verarbeitet werden.

2.2 Iron Mountain kann als für die Verarbeitung Verantwortlicher personenbezogene Daten der Mitarbeiter des Kunden und seiner verbundenen Unternehmen für legitime Geschäftszwecke, wie z. B. Vertrags- und Kundenbeziehungsmanagement, und in Übereinstimmung mit der Datenschutzgesetzgebung und den Datenschutzhinweisen von Iron Mountain, die auf den Websites von Iron Mountain verfügbar sind, sowie anderen geltenden Datenschutzrichtlinien erfassen und verarbeiten. Die in dieser DPA festgelegten Verpflichtungen von Iron Mountain gelten nicht für die Verarbeitung solcher personenbezogenen Daten.

2.3 Der Gegenstand der Verarbeitung personenbezogener Daten ist die Erbringung der Dienstleistungen. Die Rechte und Pflichten des Kunden und Iron Mountain sind in dieser DPA festgelegt. Anhang 1 dieser DSGVO beschreibt die Art, die Dauer und den Zweck der Verarbeitung, die Arten der personenbezogenen Kundendaten, die Iron Mountain verarbeitet, und die Kategorien der betroffenen Personen, deren personenbezogene Daten verarbeitet werden.

2.4 Wenn Iron Mountain im Rahmen der Erbringung der Dienstleistungen personenbezogene Daten des Kunden verarbeitet, wird Iron Mountain diese verarbeiten:

2.4.1 die persönlichen Daten des Kunden nur in Übereinstimmung mit den dokumentierten Anweisungen des Kunden zu verarbeiten. Wenn Iron Mountain gesetzlich verpflichtet ist, die personenbezogenen Daten des Kunden für einen anderen Zweck zu verarbeiten, wird Iron Mountain den Kunden zuerst benachrichtigen, es sei denn, das Gesetz bzw. die Gesetze verbieten dies aus wichtigen Gründen des öffentlichen Interesses; und

2.4.2 Halten Sie stets die geltenden Datenschutzgesetze ein und benachrichtigen Sie den Kunden unverzüglich, wenn eine vom Kunden erteilte Anweisung zur Verarbeitung personenbezogener Kundendaten nach Ansicht von Iron Mountain gegen die geltenden Datenschutzgesetze verstößt.

2.5 Iron Mountain ist an die Anweisungen des Kunden gebunden, es sei denn, die Ausführung der Anweisungen erfordert die Erbringung einer Dienstleistung im Rahmen des Vertrags und der Kunde weigert sich, die Dienstleistungsgebühren für diese Dienstleistungen zu zahlen.

2.6 Iron Mountain ergreift angemessene Maßnahmen, um die Zuverlässigkeit und Kompetenz des Personals von Iron Mountain zu gewährleisten, das Zugang zu den personenbezogenen Daten des Kunden hat, und stellt sicher, dass das Personal, das Zugang zu den personenbezogenen Daten des Kunden benötigt, einer verbindlichen Verpflichtung zur Vertraulichkeit in Bezug auf diese personenbezogenen Daten des Kunden unterliegt.

3. HILFESTELLUNG FÜR DEN KUNDEN

3.1 Iron Mountain wird den Kunden unter Berücksichtigung der Art der Verarbeitung unterstützen:

3.1.1 durch die Ergreifung geeigneter technischer und organisatorischer Maßnahmen und, soweit möglich, durch die Erfüllung der Verpflichtungen des Kunden zur Beantwortung von Anfragen von betroffenen Personen, die ihre Rechte ausüben;

3.1.2 bei der Sicherstellung der Einhaltung der Verpflichtungen des Kunden (z. B. Sicherheit der Verarbeitung, Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Mitteilung einer Verletzung des Schutzes personenbezogener Daten an die betroffene Person, Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörden, wenn die Verarbeitung ohne Maßnahmen des für die Verarbeitung Verantwortlichen zur Risikominderung zu einem hohen Risiko führen würde), wobei die Iron Mountain vorliegenden Informationen berücksichtigt werden;

und

3.1.3 indem er dem Kunden alle Informationen zur Verfügung stellt, die der Kunde vernünftigerweise anfordert, um nachzuweisen, dass seine Verpflichtungen bei der Auswahl und Beauftragung von Iron Mountain erfüllt wurden.

4. MASSNAHMEN ZUR SICHERHEIT

4.1 Unter Berücksichtigung der üblichen Betriebsverfahren, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung setzt Iron Mountain geeignete und angemessene technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten des Kunden sowie zum Schutz der personenbezogenen Daten des Kunden vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor versehentlichem Verlust, Zerstörung, Beschädigung, Änderung oder Vernichtung um. Die Sicherheitsstandards von Iron Mountain sind in Anhang 2 zu dieser DPA aufgeführt.

4.2 Es liegt in der alleinigen Verantwortung des Kunden, zu prüfen, ob diese technischen und organisatorischen Maßnahmen den Anforderungen des Kunden genügen.

5. EINHALTUNG VON GESETZEN

Der Kunde und seine verbundenen Unternehmen müssen: (i) die personenbezogenen Daten des Kunden in Übereinstimmung mit den Datenschutzgesetzen verarbeiten; (ii) befugt sein, Iron Mountain schriftliche Anweisungen zur Verarbeitung der personenbezogenen Daten des Kunden in Verbindung mit den Dienstleistungen zu erteilen (auch im Namen eines Dritten, der für die personenbezogenen Daten des Kunden verantwortlich ist); und (iii) jederzeit die Kontrolle und Befugnis über die personenbezogenen Daten des Kunden in Verbindung mit den Dienstleistungen behalten.

6. SUB-BEARBEITUNG

6.1 Der Kunde erkennt an und erklärt sich damit einverstanden, dass Iron Mountain seine Muttergesellschaft, verbundene Unternehmen und andere Drittverarbeiter (einschließlich Drittverarbeiter, die von Iron Mountains verbundenen Unternehmen oder der Muttergesellschaft beauftragt wurden) für die Zwecke der Verarbeitung personenbezogener Kundendaten im Rahmen dieser DSGVO vorbehaltlich der nachstehenden Klausel 6.2 beauftragen kann.

6.2 Eine Liste der Unterauftragsverarbeiter, denen der Kunde zum Zeitpunkt dieser DPA zugestimmt hat, finden Sie hier[1]. Iron Mountain kann den Unterauftragsverarbeiter jederzeit ersetzen oder einen neuen Unterauftragsverarbeiter ernennen, sofern der Kunde fünfzehn (15) Tage im Voraus schriftlich benachrichtigt wird und nicht innerhalb dieses Zeitraums aus nachweisbaren datenschutzrechtlichen Gründen Einspruch gegen solche Änderungen erhebt. Um diese E-Mail-Benachrichtigungen zu erhalten, muss der Kunde ein bestehendes Abonnement für den Benachrichtigungsdienst von Iron Mountain über diese Webseite abonnieren und verwalten[2].

6.3 Wenn der Kunde diesen Benachrichtigungsdienst nicht abonniert, haftet Iron Mountain nicht für die fehlende Benachrichtigung des Unterauftragsverarbeiters, und es wird davon ausgegangen, dass alle derartigen Bestellungen vom Kunden genehmigt wurden. Iron Mountain bemüht sich in angemessener Weise, dem Kunden eine Änderung der Dienste zur Verfügung zu stellen oder eine Änderung der Konfiguration oder Nutzung der Dienste durch den Kunden zu empfehlen, wenn der Kunde innerhalb von fünfzehn (15) Tagen vor der schriftlichen Benachrichtigung aus nachweisbaren Gründen im Zusammenhang mit dem Datenschutz schriftlich widerspricht. Nach Prüfung und Genehmigung durch den Kunden darf der beanstandete Unterauftragsverarbeiter keine personenbezogenen Daten des Kunden verarbeiten. Stimmt der Kunde den von Iron Mountain vorgeschlagenen Änderungen nicht innerhalb von fünfzehn (15) Tagen zu, kann Iron Mountain den Dienst oder den Teil des Dienstes, der von Iron Mountain nicht ohne die Verwendung des beanstandeten Unterauftragsverarbeiters erbracht werden kann, durch schriftliche Mitteilung an den Kunden sofort beenden. Alle Rechte und Verbindlichkeiten der Parteien bleiben von einer solchen Beendigung unberührt, vorausgesetzt, dass Iron Mountain oder eines der verbundenen Unternehmen von Iron Mountain für eine solche Beendigung keine Kündigungsgebühren, Auslagen oder sonstigen Entschädigungen berechnet. Vorbehaltlich der Vertragsbedingungen und auf Kosten des Kunden nimmt der Kunde die Vermögenswerte, die er Iron Mountain als Teil der gekündigten Dienste zur Verfügung gestellt hat, unverzüglich in Besitz.

6.4 Wie in den geltenden Datenschutzgesetzen vorgeschrieben, stellt Iron Mountain sicher, dass alle Verträge mit Unterauftragsverarbeitern, die in den Geltungsbereich dieser DSGVO fallen, dieselben Bestimmungen enthalten wie die in dieser DSGVO. Im Falle eines Verstoßes gegen diese DPA oder geltende Datenschutzgesetze durch einen Unterauftragsverarbeiter von Iron Mountain bleibt Iron Mountain gegenüber dem Kunden voll haftbar.

7. BRÜCHE IN DER SICHERHEIT

7.1 Im Falle eines vermuteten Sicherheitsverstoßes wird Iron Mountain:

7.1.1 unverzüglich Maßnahmen zu ergreifen, um die mutmaßliche Sicherheitsverletzung zu untersuchen, die Auswirkungen der mutmaßlichen Sicherheitsverletzung zu ermitteln, zu

verhindern und abzumildern und die Sicherheitsverletzung zu beheben;

7.1.2 Sobald er einen angemessenen Grad an Gewissheit hat, dass eine Sicherheitsverletzung vorliegt, muss er den Kunden unverzüglich benachrichtigen und ihm eine detaillierte Beschreibung der Sicherheitsverletzung zur Verfügung stellen, einschließlich aller Informationen, die der Kunde vernünftigerweise benötigt, um seinen Meldepflichten gemäß den Datenschutzgesetzen nachzukommen.

7.2 Der Kunde erklärt sich damit einverstanden, dass Iron Mountain die in Abschnitt 7.1.2 geforderten Informationen schrittweise bereitstellen kann. In den Fällen, in denen Iron Mountain keinen Zugang zu bestimmten Informationen hat oder diese nicht bereitstellen kann, die in Klausel 7.1.2 an den Kunden, so wird Iron Mountain den Kunden entsprechend informieren, und Iron Mountain übernimmt keine Haftung für die Nichtbereitstellung solcher Informationen.

[1] https:// www.ironmountain.com/-/media/files/Utility/Legal/GLOBAL-Personal-Data-Subprocessors-List.xlsx?la=en [2] https://urldefense.proofpoint.com/v2/url?u=https-3A reach.ironmountain. com_LegalSubprocessorSubscription&d=DwMFaQ&c=jxhwBfk-KSV6FFIot0PGng&r=JTlzF2zjl-gYEq5GmWmZcbgd-- hqyVuleEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8Aa_U6-YibdZ3Yg_2F68&s=xNzeKlzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

8. AUDITS

Iron Mountain gestattet dem Kunden und seinen jeweiligen Wirtschaftsprüfern oder bevollmächtigten Vertretern die Durchführung von Prüfungen oder Inspektionen während der Vertragslaufzeit, sofern Iron Mountain dies mindestens zehn (10) Werktage vorher ankündigt, vorausgesetzt, dass Iron Mountain nicht verpflichtet ist, Informationen über (i) andere Kunden von Iron Mountain, (ii) nichtöffentliche externe Berichte von Iron Mountain und (iii) interne Berichte, die von der internen Rechnungsprüfung oder der Compliance-Funktion von Iron Mountain erstellt wurden, zur Verfügung zu stellen oder den Zugang zu diesen zu gestatten. Eine gemäß dieser Klausel durchgeführte Prüfung oder Inspektion beschränkt sich darauf, sicherzustellen, dass Iron Mountain die personenbezogenen Kundendaten in Übereinstimmung mit seinen Verpflichtungen gemäß dieser DSGVO verarbeitet. Außer im Falle eines Sicherheitsverstoßes wird innerhalb eines Zeitraums von zwölf (12) Monaten nicht mehr als eine solche Prüfung durchgeführt.

9. INTERNATIONALE DATENÜBERMITTLUNG (EINGESCHRÄNKTE ÜBERMITTLUNG)

9.1 Soweit zutreffend, stimmt der Kunde der internationalen Übermittlung personenbezogener Kundendaten an die in Abschnitt 6.2 und in Übereinstimmung mit Anhang 3 aufgeführten Einrichtungen zur Erbringung der Dienstleistungen zu und genehmigt diese, und der Kunde und Iron Mountain stimmen dem zu:

9.1.1 die geltenden Datenschutzgesetze im Hinblick auf solche Übermittlungen einzuhalten;

9.1.2 dass sie unter Berücksichtigung, ohne Einschränkung, i) der Kategorien der personenbezogenen Daten des Kunden, ii) der Länder, deren nationale Gesetze möglicherweise kein Schutzniveau für personenbezogene Daten bieten, das mit dem der EU/des Vereinigten Königreichs vergleichbar ist ("**Drittland**"), iii) der relevanten technischen und organisatorischen Maßnahmen gemäß Abschnitt 7 und iv) der relevanten Parteien, die an der Verarbeitung dieser personenbezogenen Daten des Kunden beteiligt sind, eine Bewertung der Angemessenheit des jeweiligen Übermittlungsmechanismus vorgenommen haben, der im Rahmen dieser DPA angenommen wurde, sofern dies gesetzlich vorgeschrieben ist, und festgestellt haben, dass dieser Übermittlungsmechanismus angemessen gestaltet ist, um zu gewährleisten, dass personenbezogene Daten, die gemäß dieser DPA übermittelt werden, im Bestimmungsland ein Schutzniveau genießen, das im Wesentlichen dem durch die Datenschutzgesetzgebung garantierten Schutzniveau entspricht.

10. HAFTUNG UND ENTSCHÄDIGUNG

10.1 Im Falle einer Sicherheitsverletzung, die unmittelbar durch eine Verletzung der Verpflichtungen von Iron Mountain im Rahmen dieser DPA verursacht wurde, erstattet Iron Mountain dem Kunden in dem nach geltendem Recht zulässigen Umfang die direkten, nachweisbaren, notwendigen und angemessenen Kosten, die dem Kunden durch Dritte entstanden sind, um (a) eine solche Sicherheitsverletzung zu untersuchen,
(b) die Erstellung und Versendung von Mitteilungen an die betroffenen Personen und die Aufsichtsbehörden gemäß den Datenschutzgesetzen, (c) die Bereitstellung von Kreditüberwachungsdiensten für diese Personen gemäß den gesetzlichen Bestimmungen für einen Zeitraum von höchstens zwölf (12) Monaten und (d) die Zahlung des Anteils der von einer Aufsichtsbehörde auferlegten Geldbußen, Strafen oder Sanktionen, für die Iron Mountain nach Angaben der Aufsichtsbehörde direkt verantwortlich ist.

10.2 Für den Fall, dass eine betroffene Person eine oder beide Parteien wegen einer angeblichen Verletzung der Datenschutzgesetze verklagt ("**Ansprüche der betroffenen Person**"), wo dies zulässig ist, hat jede Partei ihre eigene Verteidigung gegen eine solche Klage (oder ihren Teil der Verteidigung) zu kontrollieren und bleibt allein verantwortlich für ihre eigenen Kosten, Ausgaben und Verbindlichkeiten in diesem Zusammenhang, einschließlich Anwaltsgebühren oder Beträge, die ihr von einem Gericht zugesprochen oder von ihr im Rahmen eines Vergleichs gezahlt wurden, Wenn jedoch jede Partei für einen Teil oder eine der Parteien für den gesamten Schaden verantwortlich ist, den eine betroffene Person aufgrund desselben Vorfalls oder derselben Reihe von Vorfällen erlitten hat, und die betroffene Person nur von einer Partei (der "**entschädigenden Partei**") vollständigen Schadenersatz erhalten hat, ist die entschädigende Partei berechtigt, von der anderen Partei den Teil des Schadenersatzes zurückzufordern, der dem von dieser anderen Partei verursachten Schaden entspricht. Nach geltendem Recht kann die Entschädigungspartei ihren Anspruch gegenüber der anderen Partei nur innerhalb von 12 Monaten nach dem Vorfall geltend machen.

10.3 Für alle Ansprüche des Kunden, die sich aus diesem DPA und/oder dem Vertrag gegen Iron Mountain ergeben oder damit in Zusammenhang stehen, gelten die Haftungsbeschränkungen und Schadensersatzausschlüsse, die im Vertrag festgelegt sind, für die Gesamthaftung. Es bestehen Haftungsbeschränkungen und Schadensersatzausschlüsse für alle Ansprüche, unabhängig davon, ob sie auf einem Vertrag, einer unerlaubten Handlung oder einer anderen Haftungstheorie beruhen, und alle Verweise auf die Haftung von Iron Mountain beziehen sich auf die kombinierte Haftung von Iron Mountain und allen mit Iron Mountain verbundenen Unternehmen für Ansprüche des Kunden und anderer mit dem Kunden verbundener Unternehmen. Soweit dies nach geltendem Recht erforderlich ist, ändert oder beschränkt dieser Abschnitt nicht (i) die Haftung der Parteien für Ansprüche der betroffenen Person, die

gegen eine Partei erhoben werden, wenn eine gesamtschuldnerische Haftung besteht, oder (ii) die Verantwortung einer Partei für die Zahlung von Strafen, die von einer Aufsichtsbehörde gegen diese Partei verhängt werden.

10.4 Für Verluste, Schäden, Kosten oder Haftungen im Zusammenhang mit dieser DPA sind die Klauseln 10.1 bis 10.3 das einzige und ausschließliche Rechtsmittel jeder Partei.

11. ERSUCHEN UM ERTEILUNG ÖFFENTLICHER GEWALT

11.1 In Übereinstimmung mit den nachstehenden Abschnitten 11.2 bis 11.5 informiert Iron Mountain den Kunden, wenn:

11.1.1 eine rechtsverbindliche Aufforderung zur Offenlegung personenbezogener Kundendaten, die gemäß dem Abkommen übermittelt wurden, von einer Behörde, einschließlich Justizbehörden, nach dem Recht des Bestimmungslandes erhält; oder

11.1.2 Kenntnis von einem direkten Zugriff öffentlicher Behörden auf personenbezogene Daten des Kunden erhält, die gemäß dem Vertrag und in Übereinstimmung mit den Gesetzen des Ziellandes übermittelt wurden.

11.2 Iron Mountain bemüht sich nach besten Kräften, eine Aufhebung des Verbots zu erwirken, wenn die Gesetze des Bestimmungslandes eine Benachrichtigung des Kunden nicht zulassen.

11.3 Neben der Prüfung der Rechtmäßigkeit des Offenlegungsantrags erklärt sich Iron Mountain auch bereit, den Antrag anzufechten, wenn es zu dem Schluss kommt, dass der Antrag nach den Gesetzen des Bestimmungslandes rechtswidrig ist, und insbesondere zu prüfen, ob der Antrag im Rahmen der Befugnisse der ersuchenden öffentlichen Behörde bleibt. Die angeforderten personenbezogenen Kundendaten werden nicht weitergegeben, es sei denn, dies ist nach den geltenden Verfahrensvorschriften erforderlich.

11.4 Auf der Grundlage einer angemessenen Auslegung des Antrags erklärt sich Iron Mountain bereit, das zulässige Mindestmaß an Informationen zur Verfügung zu stellen.

11.5 Auf Anfrage stellt Iron Mountain die Informationen der zuständigen Aufsichtsbehörde für die Dauer der Vereinbarung zur Verfügung.

12. VERSCHIEDENES

12.1 Bei Beendigung/Ablauf der Vereinbarung wird Iron Mountain auf der Grundlage der spezifischen Anweisungen des Kunden und in Übereinstimmung mit den Bedingungen der Vereinbarung alle personenbezogenen Daten des Kunden entweder löschen/vernichten oder an den Kunden oder an einen vom Kunden benannten Dritten zurückgeben, je nach Art der von Iron Mountain erbrachten Dienstleistungen. Wie in der Vereinbarung oder in einem anderen anwendbaren Vertragsdokument festgelegt, werden alle personenbezogenen Daten des Kunden, die sich im Besitz des Kunden befinden, im Rahmen eines vereinbarten Ausstiegs- oder Übergangsplans und zu den vereinbarten Kosten an den Kunden zurückgegeben. In allen anderen Fällen, in denen der Vertrag keine Angaben zur Löschung/Vernichtung oder Rückgabe der personenbezogenen Daten des Kunden enthält und der Kunde innerhalb von fünfzehn (15) Tagen nach Beendigung/Ablauf des Vertrags keine Anweisungen zur Löschung/Vernichtung oder Rückgabe der personenbezogenen Daten des Kunden erteilt, sendet Iron Mountain eine schriftliche Mitteilung an den Kunden, in der er aufgefordert wird, innerhalb von 15 (fünfzehn) Tagen spezifische Anweisungen zur Löschung/Vernichtung oder Rückgabe der personenbezogenen Daten des Kunden zu erhalten, und in der er den Kunden über alle anfallenden Gebühren für die sichere Vernichtung oder andere vom Kunden zu zahlende Gebühren informiert. Ein Kunde, der es versäumt, innerhalb von fünfzehn (15) Tagen nach Beendigung des Vertrags schriftliche Anweisungen zu erteilen und die entsprechenden Gebühren innerhalb dieses Zeitraums zu zahlen, ermächtigt Iron Mountain hiermit, alle personenbezogenen Daten des Kunden nach dem Ermessen von Iron Mountain und auf Kosten des Kunden nach Beendigung des Vertrags weiter zu verarbeiten, zu löschen und zu vernichten.

12.2 Trotz Klausel 12.1 haftet Iron Mountain nicht für das Versäumnis, personenbezogene Kundendaten, die auf Sicherungsbändern gespeichert sind, zu löschen, solange diese während des normalen Geschäftsbetriebs überschrieben werden (und die personenbezogenen Kundendaten gelöscht werden).

12.3 Mit Ausnahme der Standardvertragsklauseln (wie in Anhang 3 zu dieser DPA definiert) unterliegen diese DPA und alle Streitigkeiten, Ansprüche oder Meinungsverschiedenheiten, die sich aus oder im Zusammenhang mit dieser DPA oder ihrer Verletzung, Beendigung oder Gültigkeit ergeben, der Rechtswahlklausel der Vereinbarung; und alle Streitigkeiten, Meinungsverschiedenheiten oder Ansprüche, die sich aus oder im Zusammenhang mit dieser DPA ergeben, werden in erster Linie durch ein in der Vereinbarung festgelegtes Streitbeilegungsverfahren beigelegt.

12.4 Jede Partei kann der anderen Partei schriftlich alle Änderungen dieser DPA mitteilen, die ihrer Ansicht nach erforderlich sind, um den Anforderungen der Datenschutzgesetze oder einer Entscheidung einer

Aufsichtsbehörde oder eines zuständigen Gerichts gerecht zu werden. Solche Änderungen werden nur wirksam, wenn und soweit sie in einer von beiden Parteien unterzeichneten einvernehmlichen Änderung dieser DPA festgelegt sind, es sei denn, eine Partei informiert die andere Partei über eine neue gesetzliche Vorschrift und sendet eine solche Änderung, die nur die notwendigen Änderungen enthält und ohne förmliche Zustimmung akzeptiert werden kann, d. h. wenn innerhalb einer bestimmten Frist kein Widerspruch erhoben wird, als einvernehmliche Änderung dieser DPA.

ANHANG 1

Angaben zur Verarbeitung und Datenübermittlung (falls zutreffend)

A. LISTE DER PARTEIEN:

Die Parteien dieser DPA sowie die Rollen des Datenexporteurs und des Datenimporteurs sind in dem Abkommen und gegebenenfalls in Anhang 3 (Internationale Datenübermittlung) aufgeführt.

B. BESCHREIBUNG DER VERARBEITUNG/ÜBERTRAGUNG (fallszutreffend):

Kategorien von betroffenen Personen, deren personenbezogene Daten verarbeitet/übertragen werden:

Der Kunde kann Iron Mountain personenbezogene Daten verschiedener Kategorien von betroffenen Personen übermitteln, je nach der Art der Dienstleistungen von Iron Mountain und der Geschäftstätigkeit des Kunden, deren Umfang der Kunde nach eigenem Ermessen bestimmt und kontrolliert. Zu den Kategorien betroffener Personen gehören: frühere und derzeitige Mitarbeiter, frühere und derzeitige Auftragnehmer oder Berater, von Agenturen beauftragte Auftragnehmer oder Berater und externe Hilfskräfte, Stellenbewerber und -Kandidaten, Studenten und Freiwillige, Personen, die von Mitarbeitern oder Rentnern als Begünstigte, Ehegatten, Lebenspartner, Angehörige und Kontaktpersonen für Notfälle angegeben werden, Rentner, frühere und derzeitige Direktoren und leitende Angestellte, Aktionäre, Anleihegläubiger, Kontoinhaber, Endnutzer/Verbraucher (Erwachsene, Kinder), Patienten (Erwachsene, Kinder), Passanten (Überwachungskameras) und Website-Nutzer.

Kategorien der verarbeiteten/übertragenen personenbezogenen Daten:

Je nach Art der Dienstleistungen von Iron Mountain und der Geschäftstätigkeit des Kunden kann der Kunde Iron Mountain personenbezogene Daten übermitteln, die zu verschiedenen Kategorien personenbezogener Daten gehören, deren Umfang der Kunde nach eigenem Ermessen bestimmt und kontrolliert. Diese Kategorien können personenbezogene Daten über den Kunden und/oder seine eigenen Kunden, Mitarbeiter usw. umfassen.

Übermittlung sensibler Daten (falls zutreffend):

Je nach Art der Dienstleistungen von Iron Mountain und der Geschäftstätigkeit des Kunden kann der Kunde sensible Daten an Iron Mountain übermitteln, deren Umfang der Kunde nach eigenem Ermessen bestimmt und kontrolliert.

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

Die Übertragung erfolgt laufend.

Art der Verarbeitung:

Sammlung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Veränderung, Abruf, Abfrage, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder sonstige Bereitstellung, Abgleich oder Kombination, Einschränkung, Löschung oder Vernichtung.

Zweck(e) der Datenverarbeitung/Übermittlung (falls zutreffend) und Weiterverarbeitung:

Die Erbringung von Dienstleistungen in Übereinstimmung mit den Bestimmungen des Vertrags.

Vorratsspeicherung von Daten:

Iron Mountain bewahrt die personenbezogenen Daten für die Dauer der für den Kunden erbrachten Dienstleistungen und bis zur Rückgabe oder Vernichtung der personenbezogenen Daten gemäß Abschnitt 10.1 dieser DSGVO auf.

Gegebenenfalls Angabe des Gegenstands, der Art und der Dauer der Verarbeitung bei Übermittlungen an (Unter-)Auftragsverarbeiter:

Die Unterauftragsverarbeiter erbringen für die Dauer des Vertrags mit dem Kunden IT- und Beratungsdienste, einschließlich globaler IT-Unterstützung, Ereignisberichterstattung und Managementdienste.

C. FACHKUNDIGE AUFSICHTSBEHÖRDE

Wie in Anhang 3 (Internationale Datenübermittlung) angegeben, falls zutreffend.

ANHANG 2

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ("SICHERHEITSMASSNAHMEN")

1. INFORMATIONSSICHERHEIT PROGRAMM UND -POLITIK

Iron Mountain muss ein Informationssicherheitsprogramm unterhalten, das angemessene physische, technische und administrative Kontrollen umfasst, die den Industriestandards entsprechen. Die folgenden Punkte müssen in das Informationssicherheit Programm aufgenommen werden:

1.1 Die Richtlinien, Standards und Verfahren zur Informationssicherheit von Iron Mountain werden dokumentiert, intern veröffentlicht und kommuniziert;

1.2. Dokumentierte, klare Zuweisung von Verantwortung und Befugnissen für die Erstellung und Pflege des Informationssicherheitsprogramms;

1.3 Regelmäßige Tests der wichtigsten Kontrollen, Systeme und Verfahren des Informationssicherheitsprogramms;

1.4 Es bestehen administrative, technische und betriebliche Sicherheitsvorkehrungen zum Schutz aller personenbezogenen Kundendaten gemäß den in diesem Sicherheitsanhang beschriebenen Praktiken, Verfahren und Prozessen, soweit sie für das Format, in dem die personenbezogenen Kundendaten gespeichert sind, relevant und anwendbar sind.

2. BEWERTUNG DES RISIKOS

Iron Mountain ist verpflichtet, ein Programm zur Bewertung von Informationssicherheitsrisiken zu unterhalten, das vernünftigerweise vorhersehbare interne und externe Risiken und Schwachstellen identifiziert und bewertet, die Sicherheit, Vertraulichkeit und/oder Integrität der persönlichen Kundendaten gefährden könnten. Jährlich oder immer dann, wenn sich das Risiko oder die Anfälligkeit für personenbezogene Kundendaten wesentlich ändert, bewertet Iron Mountain die Wirksamkeit des aktuellen Informationssicherheitsprogramms zur Begrenzung solcher Risiken und aktualisiert es, soweit dies erforderlich, angemessen und geeignet ist.

3. VERWALTUNG VON INFORMATIONSVERARBEITUNG ANLAGEN UND PHYSISCHEN MEDIEN

3.1 Verwaltung von Informationsverarbeitung Anlagen. Iron Mountain verfügt über ein Programm zur Verwaltung des Anlageninventars, um die physischen, technischen und administrativen Kontrollen seiner Informationsverarbeitungsanlagen (wie Computer, Server, Speichergeräte, Kommunikationsnetze, PCs, Laptops und Peripheriegeräte) zu verwalten.

Das Programm zur Verwaltung des Anlageninventars umfasst folgende Bereiche:

3.1.1 Den Mitarbeitern von Iron Mountain wurden die Eigentumsrechte an den Vermögenswerten schriftlich zugewiesen, um eine angemessene Klassifizierung der Informationen, die Festlegung der Zugangsbeschränkungen und die Überprüfung der Zugangskontrollen sicherzustellen.

3.1.2 Säuberung von Vermögenswerten vor der Entsorgung gemäß NIST 800-88.

3.1.3 Bevor Geräte oder Software, die nicht einer bestimmten Person zugewiesen sind, aus den Räumlichkeiten von Iron Mountain entfernt werden können, ist eine Genehmigung der Geschäftsleitung erforderlich.

3.2 Kontrolliert. Iron Mountain verfügt über die folgenden Kontrollen:

3.2.1 Betriebsverfahren und technische Kontrollen zum Schutz von Dokumenten, Computermedien, Eingabe-/Ausgabe-/Sicherungsdaten und Systemdokumentation vor unbefugter Offenlegung, Änderung und Zerstörung.

3.2.2 Verfahren zur sicheren Entsorgung elektronischer oder physischer Datenträger, die personenbezogene Kundendaten enthalten.

3.2.3 Ein etabliertes Verfahren zur Nachverfolgung aller physischen Datenträger des Kunden von dem Zeitpunkt an, an dem sie in die Obhut von Iron Mountain gelangen, bis zu ihrer endgültigen Entnahme oder Vernichtung.

4. MASSNAHMEN ZUR SICHERHEIT DER MITARBEITER

4.1 Vertraulichkeit. Iron Mountain verlangt in angemessener Weise, dass alle Mitarbeiter von Iron Mountain, einschließlich der Zeit- und Vertragsangestellten, sich verpflichten, die persönlichen Kundendaten vertraulich zu behandeln und die internen Richtlinien von Iron Mountain zur Informationssicherheit und zur akzeptablen Nutzung zu befolgen.

4.2 Politik der Hintergrunduntersuchung. Iron Mountain hat eine Richtlinie für Hintergrunduntersuchungen und Drogentests (nur in den Vereinigten Staaten) für seine Mitarbeiter in Kraft gesetzt. Iron Mountain wird diese Politik für die Dauer des Abkommens beibehalten. Zu den Anforderungen gehören u. a. Drogenscreenings (nur in den Vereinigten Staaten), Überprüfung der Identität des Personals, Strafregisterabfragen, Überprüfungen der Beschäftigung, Abfragen der Überwachungsliste der Regierung/Terroristen, Überprüfungen der Ausbildung bestimmter Mitarbeiter sowie der Führerscheinerwerb und die Vorgeschichte von Verstößen bei Fahrerkandidaten und vorhandenen Fahrern. Wenn bei einer Zuverlässigkeitsüberprüfung nachteilige Informationen aufgedeckt werden, führt Iron Mountain eine individuelle Bewertung in Übereinstimmung mit den geltenden Arbeitsgesetzen und bewährten Praktiken durch.

4.3 Arbeit mit Unterauftragnehmern. Iron Mountain verlangt von allen Unterauftragnehmern, die Dienstleistungen im Rahmen des Vertrags erbringen, die Einhaltung ähnlicher Beschränkungen, wie sie in diesem Abschnitt dargelegt sind, in Bezug auf alle Mitarbeiter von Unterauftragnehmern, die Dienstleistungen im Rahmen des Vertrags erbringen, die Verarbeitung personenbezogener Kundendaten beinhalten.

4.4 Schulungen zum Sicherheitsbewusstsein. Iron Mountain muss allen Iron Mountain-Mitarbeitern, die Zugang zu personenbezogenen Kundendaten haben, mindestens einmal im Jahr eine allgemeine Schulung zum Sicherheitsbewusstsein sowie ein rollensbezogenes Sicherheitstraining anbieten. Iron Mountain führt Aufzeichnungen, in denen die Namen solcher Iron Mountain-Mitarbeiter, die anwesend waren, sowie die Daten der einzelnen Schulungen zum Sicherheitsbewusstsein. Das Schulungsprogramm von Iron Mountain zum Sicherheitsbewusstsein muss regelmäßig überprüft und aktualisiert werden.

4.5 Personal aus Iron Mountain abziehen. Iron Mountain unterhält ein Disziplinarverfahren für Mitarbeiter, die gegen die hier dargelegten Sicherheitsanforderungen verstoßen.

4.6 Beendigung des Zugangs bei Beendigung/Wiederzuweisung. Der Zugang eines Iron Mountain-Mitarbeiters zu den persönlichen Daten des Kunden muss bei Beendigung des Arbeitsverhältnisses oder bei einer Versetzung in eine Rolle, die keinen Zugang zu den persönlichen Daten des Kunden erfordert, unverzüglich widerrufen werden.

5. PHYSISCHE UND ÖKOLOGISCHE SICHERHEIT

5.1 Physische Sicherheitskontrollen. In den Einrichtungen von Iron Mountain werden physische Kontrollen eingesetzt, die den Zugang zu personenbezogenen Kundendaten angemessen einschränken, z. B. Zugangskontrollprotokolle, physische Barrieren wie verschlossene Einrichtungen und Bereiche, Zugangsausweise für Mitarbeiter, Besucherprotokolle, Zugangsausweise für Besucher, Kartenlesegeräte, Videoüberwachungskameras und Alarmanlagen zur Einbruchmeldung, soweit Iron Mountain dies für angemessen hält. Alle Besucher müssen sich anmelden und sind verpflichtet, sich jederzeit begleiten zu lassen.

5.2 Unterstützende Hilfsprogramme. Iron Mountain ergreift Maßnahmen, um seine Einrichtungen und Systeme, die personenbezogene Kundendaten enthalten, vor Ausfällen der Stromversorgung, der Telekommunikation, der Wasserversorgung, des Abwassers, der Heizung, der Belüftung und der Klimaanlage zu schützen, soweit dies möglich ist.

5.3 Sicherheit des Übermittlungssystems. Iron Mountain ergreift Maßnahmen, um die physische Sicherheit seiner Netzinfrastruktur und Telekommunikationssysteme vor dem Abfangen von Übertragungen und vor Schäden zu schützen.

5.4 Offsite-Ausstattung. Wenn Iron Mountain Funktionen auslagert, die den Einsatz von externen Geräten zur Unterstützung von Dienstleistungen erfordern, müssen alle externen Geräte, auf denen personenbezogene Kundendaten gespeichert sind, auf die gleiche Weise gesichert werden wie die für den gleichen Zweck verwendeten Geräte vor Ort.

5.5 Physischer Zugang zu Informationen Verarbeitungsanlagen. Iron Mountain bewahrt die Aufzeichnungen von Iron Mountain-Mitarbeitern, die berechtigt sind, physischen Zugang zu den von Iron Mountain zur Erbringung von Dienstleistungen genutzten kontrollierten Computerumgebungen zu haben, ein Jahr lang auf und gewährt dem Kunden auf dessen Anfrage im Zusammenhang mit einer Sicherheitsverletzung und vorbehaltlich der Sicherheitsrichtlinien von Iron Mountain Zugang zur Einsicht in die prüfbaren Aufzeichnungen dieser Iron Mountain-Mitarbeiter.

5.6 Der physische Zugang ist eingeschränkt. Der physische Zugang zu den von Iron Mountain kontrollierten Einrichtungen, in denen personenbezogene Kundendaten verarbeitet werden, ist auf Iron Mountain-Mitarbeiter und autorisierte Personen zu beschränken, die eine geschäftliche Notwendigkeit für diesen Zugang haben. Iron Mountain muss über ein Verfahren verfügen, um Anträge auf physischen Zugang zu solchen Einrichtungen zu genehmigen und zu verfolgen.

5.7 Reparaturen und Änderungen. Iron Mountain führt Aufzeichnungen über alle sicherheitsrelevanten Reparaturen und Änderungen an physischen Komponenten, einschließlich Hardware, Wänden, Türen und Schlössern, von Sicherheitsbereichen in Einrichtungen, in denen personenbezogene Kundendaten gespeichert sind.

5.8 Aufzeichnungen. Führen Sie Aufzeichnungen über alle Bewegungen von Hardware und elektronischen Medien sowie über die Personen, die für sie verantwortlich sind.

6. MANAGEMENT VON KOMMUNIKATIONS- UND INFORMATIONSVERARBEITUNGSPROZESSEN

6.1 Normen zur Gerätekonfiguration. Iron Mountain entwickelt, implementiert und pflegt branchenübliche Systemverwaltungsverfahren, einschließlich, aber nicht beschränkt auf, Systemhärtung, System- und Geräte-Patching (Betriebssystem und Anwendungen) sowie die ordnungsgemäße Installation und Aktualisierung von Virenschutzprogrammen.

6.2 Änderungskontrolle bei Informationsverarbeitungssystemen.. Iron Mountain verfügt über ein internes formelles Verfahren zur Beantragung von Änderungen für Informationsverarbeitungs- und Kommunikationsnetzwerksysteme, und alle neuen Informationsverarbeitungs- oder Netzwerkkommunikationsfähigkeiten, Systempatches oder Änderungen an bestehenden Systemen müssen dokumentiert, getestet und genehmigt werden, bevor neue Informationsverarbeitungs- oder Netzwerkkommunikationsfähigkeiten, Systempatches oder Änderungen an bestehenden Systemen eingeführt werden.

6.3 Trennung der Zuständigkeiten. Iron Mountain sorgt für eine Trennung der Aufgaben und

Verantwortungsbereiche, so dass keine einzelne Person die alleinige Befugnis hat, Informationsverarbeitungssysteme zu ändern, die auf personenbezogene Kundendaten zugreifen.

6.4 Trennung von Entwicklungs- und Produktionsumgebungen. Die Entwicklungs-, Test- und Produktionsumgebungen von Iron Mountain für Informationsverarbeitungssysteme müssen logisch oder physisch getrennt sein.

6.5 Management der technischen Architektur. Iron Mountain führt ein Konfigurationsmanagementverfahren ein, um die Komponenten des Informationsverarbeitungssystems und der technischen Infrastruktur, die zur Erbringung der Dienstleistungen verwendet werden, zu definieren, zu verwalten und zu kontrollieren.

6.6 Erkennung von Einbrüchen. Iron Mountain überwacht die Computersysteme und -Prozesse kontinuierlich auf versuchte oder tatsächliche Sicherheitsverletzungen und benachrichtigt den Kunden, wenn ein unbefugter Zugriff auf die persönlichen Daten des Kunden erfolgt.

6.7 Netzwerk-Sicherheit. Iron Mountain stellt sicher, dass Folgendes vorhanden ist:

6.7.1 In Bezug auf die von Iron Mountain gehostete(n) Umgebung(en), die für die Erbringung der Dienstleistungen verwendet wird (werden), melden Netzwerk-Intrusion-Detection-Systeme ("IDS") und Intrusion-Prevention-Sensoren ("IPS") Ereignisse, und es werden tägliche Berichte zur Überprüfung ausgegeben (zusammenfassend als "IDS/IPS" bezeichnet);

6.7.2 In Bezug auf die von Iron Mountain gehostete(n) Umgebung(en), die für die Erbringung der Dienstleistungen verwendet wird/werden, IDS/IPS, die mindestens wöchentlich, aber so schnell wie möglich nach Erhalt der Aktualisierungen aktualisiert werden, und die sofortige Ausführung der neuesten Bedrohungssignaturen oder -regeln;

6.7.3 Risikoreiche Ports an Systemen, die nach außen gerichtet sind, sind nicht über das Internetzugänglich;

6.7.4 Die Netzwerkverbindungen von Iron Mountain werden protokolliert und in Protokolldateien aufgezeichnet;

6.7.5 Einsatz von Firewalls zum Schutz und zur Überprüfung des gesamten ein- und ausgehenden Datenverkehrs zwischen bestimmten Netzpunkten;

6.7.6 Verhärtungsrichtlinien zur Definition von ein- und ausgehenden Netzwerkports oder Dienstverkehr für alle Iron Mountain-eigenen oder verwalteten Systeme, die als Teil des Informationssicherheitsprogramms dokumentiert und autorisiert wurden;

6.7.7 Netzwerk- und Diagnoseanschlüsse, die ordnungsgemäß gesichert sind; und

6.7.8 Richtlinien, Verfahren und technische Kontrollen zur Verhinderung, Erkennung und Beseitigung von bösartigem Code oder bekannten Angriffen auf die Informationssysteme von Iron Mountain.

6.8 Verschlüsselte Authentifizierung Nachweise. Iron Mountain muss sicherstellen, dass die Authentifizierungsdaten, die über seine Netzwerkgeräte gesendet werden, während der Übertragung verschlüsselt werden.

6.9 Sichere Netzwerk-Administration. Die Netzwerke von Iron Mountain müssen in angemessener Weise verwaltet und kontrolliert werden, um vor bekannten Bedrohungen zu schützen und die Sicherheit aller von Iron Mountain verwalteten Anwendungen und Daten im Netzwerk oder bei der Übertragung über das Netzwerk zu gewährleisten. Um unbeschränkte Verbindungen zu nicht vertrauenswürdigen Netzen oder öffentlich zugänglichen Servern zu verhindern, müssen technische Kontrollen und sichere Kommunikationsprotokolle eingesetzt werden.

6.10 Virenschutz. Iron Mountain implementiert und pflegt ein Virenschutzprogramm, einschließlich Malware-Schutz, aktueller Signaturdateien oder alternativen Schutzes gegen neu auftretende Bedrohungen, Patches und Virendefinitionen, für von Iron Mountain verwaltete Server und Workstations, die zur Speicherung von oder zum Zugriff auf personenbezogene Kundendaten verwendet werden.

6.11 Website - Client-Verschlüsselung. Iron Mountain muss sicherstellen, dass Secure Sockets Layering (SSL) aktiviert ist und dass jede seiner Websites über ein gültiges SSL-Zertifikat verfügt, das Vertraulichkeits-, Authentifizierungs- oder Autorisierungskontrollen erfordert.

6.12 Sicherung der Informationen. Iron Mountain erstellt geeignete Sicherungskopien der Systemdateien. Darüber hinaus muss Iron Mountain Verfahren für die Wiederherstellung im Katastrophenfall entwickeln und beibehalten; weitere Informationen finden Sie im Abschnitt "Wiederherstellung im Katastrophenfall" weiter unten.

6.13 Elektronische Informationen im Transit. Zum Schutz der persönlichen Kundendaten, die über öffentliche Netze übertragen werden, wenn sie von der von Iron Mountain gehosteten Infrastruktur stammen, verwendet Iron Mountain eine Verschlüsselung mit einem Industriestandardalgorithmus mit einer Schlüssellänge von mindestens 128 Bit.

6.14 Kryptographische Kontrollen. Iron Mountain befolgt eine dokumentierte Richtlinie für den Einsatz kryptografischer Kontrollen. Die kryptografischen Kontrollen von Iron Mountain sollen:

6.14.1 so konzipiert sein, dass die Vertraulichkeit und Integrität der personenbezogenen Kundendaten, die Iron Mountain in gemeinsam genutzten Netzwerkumgebungen verarbeitet, überträgt oder speichert, in Übereinstimmung mit den Bestimmungen des Vertrags angemessen geschützt werden;

6.14.2 auf personenbezogene Kundendaten angewendet werden, die über "nicht vertrauenswürdige" Netzwerke (d. h. Netzwerke, die Iron Mountain rechtlich nicht kontrolliert) übertragen werden, einschließlich derjenigen, die zum Senden von Daten an das Unternehmensnetzwerk des Kunden vom Netzwerk von Iron Mountain aus verwendet werden, vorbehaltlich der Mitwirkung des Kunden bei der Verwaltung von Verschlüsselungsschlüsseln, die zum Entschlüsseln der vom Kunden empfangenen Übertragungen erforderlich sind; und

6.14.3 Dokumentierte Praktiken zur Verwaltung von Verschlüsselungsschlüsseln, um die Sicherheit kryptographischer Technologien zu unterstützen.

6.14.4 Verschlüsselung aller persönlichen Kundendaten auf Laptops oder anderen tragbaren Geräten.

6.15 Anforderungen an die Protokollierung. Iron Mountain muss Folgendes sicherstellen:
- 6.15.1 Bedeutende Sicherheits- und Systemereignisse werden protokolliert und überprüft;
- 6.15.2 Audit-Protokolle werden mindestens ein Jahr lang für Systeme in von Iron Mountain gehosteten Umgebungen aufbewahrt, die von Iron Mountain zur Erbringung von Dienstleistungen genutzt werden;
- 6.15.3 Systemprüfungsprotokolle werden auf Anomalien überprüft; und
- 6.15.4 Die Protokollierung Einrichtungen und Systeminformationen sind in angemessener Weise vor Manipulationen und unbefugtem Zugriff geschützt.

6.16 Zeitsynchronisation im Netzwerk. Iron Mountain verwendet eine gemeinsame maßgebliche Zeitquelle, um die Systemuhren aller Informationsverarbeitungssysteme zu synchronisieren.

6.17 Abtrennung in Netzen. Iron Mountain trennt in angemessener Weise zusammengehörige Gruppen von Informationsdiensten, Benutzern und Informationssystemen in Netzen.

7. ZUGANGSKONTROLLE

7.1 Politik der Zugangskontrolle. Iron Mountain unterhält Zugangskontrolle Richtlinien in Bezug auf Informationsverarbeitung Anlagen, die von Iron Mountain formell genehmigt, veröffentlicht und umgesetzt werden.

7.2 Logische Zugriffsberechtigung. Iron Mountain muss über ein Verfahren zur Genehmigung von Anträgen auf logischen Zugang zu den persönlichen Daten des Kunden und von Anträgen auf Zugang zu den Systemen von Iron Mountain verfügen, die für die Nutzung der Dienste bestimmt sind.

7.3 Zugangskontrolle und Zugangsüberprüfung. Iron Mountain gewährt nur aktiven Iron Mountain-Mitarbeitern, einschließlich Zeit- und Vertragsmitarbeitern, und aktiven Benutzerkonten, die einen solchen Zugang zur Erfüllung ihrer Aufgaben benötigen, Zugang zu den personenbezogenen Kundendaten. Alle privilegierten Zugänge müssen vierteljährlich überprüft und bestätigt werden, dass sie mit der aktuellen Funktion übereinstimmen, und dies muss dokumentiert werden.

7.4 Kontrolle des Zugangs von Dritten. Bevor Iron Mountain externen Parteien Zugang zu den Informationssystemen von Iron Mountain gewährt, die auf personenbezogene Kundendaten zugreifen, stellt Iron Mountain sicher, dass angemessene Kontrollen vorhanden sind.

7.5 Zugangskontrolle für Betriebssysteme. Iron Mountain kontrolliert den Zugriff auf Betriebssysteme (sowohl Software als auch hardwarebasierte Betriebssysteme), indem es ein sicheres Anmeldeverfahren vorschreibt, das die Person, die auf das Betriebssystem zugreift, eindeutig identifiziert.

7.6 Mobile Computing-Geräte. Iron Mountain verfügt über eine Richtlinie oder ein Verfahren, um die mobilen Computergeräte von Iron Mountain vor unbefugtem Zugriff zu schützen. Physischer Schutz, Zugangskontrolle und Sicherheitskontrollen wie Verschlüsselung, Virenschutz und Geräte-Backup müssen in solchen Richtlinien oder Verfahren berücksichtigt werden.

7.7 Isolierung von Kundensystemen. Iron Mountain trennt die persönlichen Daten des Kunden logisch von allen anderen Informationen innerhalb der gehosteten Umgebung(en), die für die Erbringung der Dienstleistungen verwendet werden, und sorgt für deren Trennung.

7.8 Konten. Iron Mountain geht in Bezug auf die Konten wie folgt vor:
- 7.8.1 Verlangt eine Authentifizierung jedes Iron Mountain-Mitarbeiters, der versucht, Zugang zu Iron Mountain-Systemen zu erhalten, die personenbezogene Kundendaten verarbeiten, und verbietet die Verwendung gemeinsam genutzter Benutzerkonten oder von Benutzerkonten mit allgemeinen Berechtigungsnachweisen (d. h. IDs) für den Zugang zu personenbezogenen Kundendaten oder Systemen.
- 7.8.2 Verlangt, dass alle Benutzerkonto-IDs, einschließlich privilegierter Konten, direkt an eine Person (und nicht an eine Position) gebunden sind.
- 7.8.3 Verlangt die Verwendung von temporären Passwörtern, Check-Out-IDs oder ähnlichen Kontrollen für den Zugriff auf Standard-Administrationskonten, wenn die Standard-Administrationskonten nicht deaktiviert oder entfernt werden.
- 7.8.4 Inaktive reguläre Konten müssen nach 90 Tagen der Inaktivität gesperrt oder deaktiviert werden.
- 7.8.5 Verhindern Sie den Zugriff auf ein Konto nach mehreren erfolglosen Zugriffsversuchen.
- 7.8.6 Verlangt werden eindeutige Kennungen und sichere Passwörter, die mindestens folgende Merkmale aufweisen: mindestens 8 Zeichen, die alle 90 Tage geändert werden müssen und eine bestimmte Komplexität aufweisen.
- 7.8.7 Den Mitarbeitern sollte es nicht erlaubt sein,Passwörter weiterzugeben oder aufzuschreiben.

7.9 Kontrollen für unbeaufsichtigte Systeme. Iron Mountain setzt einen passwortgeschützten Bildschirmschoner für alle Systeme ein, die 30 Minuten lang unbeaufsichtigt sind und keine Aktivitäten aufweisen.

8. ENTWICKLUNG UND WARTUNG DER BESCHAFFUNG VON INFORMATIONSSYSTEMEN

8.1 Sicherheit in der Systementwicklung. Iron Mountain muss sicherstellen, dass die Sicherheit ein Teil der gesamten Entwicklung und des Betriebs von Informationssystemen ist, und es muss interne Methoden zur sicheren Kodierung auf der Grundlage von Sicherheitsstandards für die Anwendungsentwicklung veröffentlichen und befolgen.

8.2 Management der Software-Sicherheit. Die Informationssysteme von Iron Mountain (einschließlich der Betriebssysteme, der Infrastruktur, der Geschäftsanwendungen, der Dienstleistungen und der von den Benutzern entwickelten Anwendungen) müssen so konzipiert sein, dass sie den Informationssicherheitsstandards entsprechen.

8.3 Netzwerk-Diagramme. Iron Mountain ist für die Erstellung, Dokumentation und Pflege physischer und logischer Diagramme von Netzwerkgeräten und Datenverkehr zuständig.

8.4 Bewertung von Anwendung Schwachstellen/Ethical Hacking. Iron Mountain muss mindestens einmal jährlich Schwachstellenbewertungen für Anwendungen in seiner/ihren gehosteten Umgebung(en) durchführen, die zur Bereitstellung von Diensten verwendet werden, die personenbezogene Kundendaten verarbeiten. Aufgrund vertraulicher und geschützter Informationen von Iron Mountain können wir keine detaillierten Ergebnisse liefern.

8.5 Prüfung und Überprüfung von Änderungen. Vor der Bereitstellung prüft und testet Iron Mountain Änderungen an Anwendungen und Betriebssystemen, um sicherzustellen, dass es keine nachteiligen Auswirkungen auf die persönlichen Daten oder Systeme des Kunden gibt.

9. ERHOLUNG VON EINER KATASTROPHE

Iron Mountain muss einen Notfallwiederherstellungsplan vorhalten, der die Replikation von Systemen und elektronischen Daten, die zur Unterstützung der Dienste verwendet werden, in ein Backup-Rechenzentrum beinhaltet. Persönliche Kundendaten, die physisch in einer Einrichtung von Iron Mountain gespeichert sind, werden bei der Replikation von Systemen und elektronischen Daten nicht berücksichtigt. Iron Mountain wird einen Plan zur Aufrechterhaltung des Geschäftsbetriebs aufrechterhalten, um kritische Geschäftsfunktionen wiederherzustellen. Iron Mountain führt mindestens einmal alle zwölf (12) Monate Tests zur Wiederherstellung im Notfall durch.

10. EXTERNE AUDITS UND BEURTEILUNGEN

Die Sicherheitsprotokolle von Iron Mountain sind so konzipiert, dass sie den Branchenstandards entsprechen. Iron Mountain stellt dem Kunden alle unabhängigen Prüfungsberichte Dritter (z. B. PCI, ISO27001, SOC2 usw.) zur Verfügung, die für die Dienstleistungen in der Region, in der diese Dienstleistungen erbracht werden, relevant sind ("Prüfungsbericht"). Iron Mountain wird alle Berichte, die mit der Absicht in Auftrag gegeben werden, kundenorientiert zu sein, unabhängig von den Ergebnissen des Berichts zur Verfügung stellen. Iron Mountain ist nicht verpflichtet, die Ergebnisse interner Prüfungen oder die Ergebnisse anderer unabhängiger Bewertungen, die mit der Absicht in Auftrag gegeben wurden, die Informationen vertraulich zu behandeln, Iron Mountain zur Verfügung zu stellen. Kunden und

Auf Anfrage werden Kopien des Prüfungsberichts den externen Prüfern zur Verfügung gestellt. Jeder Prüfungsbericht oder jedes andere Ergebnis, das aus den in diesem Abschnitt vorgeschriebenen Tests oder Prüfungen hervorgeht, wird als vertrauliche Information von Iron Mountain betrachtet. Der Kunde hat das Recht, eine Kopie eines solchen Prüfberichts an alle Kunden oder Aufsichtsbehörden des Kunden weiterzugeben, vorbehaltlich der gleichen strengen Vertraulichkeitsbestimmungen wie die hierin festgelegten. Iron Mountain bestätigt auf Anfrage des Kunden schriftlich, dass seit der Fertigstellung eines solchen Prüfberichts keine Änderungen in den relevanten Richtlinien, Verfahren und internen Kontrollen eingetreten sind, und zwar höchstens drei Monate nach dem Ende des Berichtszeitraums des Prüfberichts.

ANHANG 3

Internationale Datenübertragungen

1. DEFINITIONEN

"**2022 UK Addendum**" bezeichnet die Vorlage Addendum B.1.0, die vom United Kingdom Information Commissioner's Office herausgegeben und dem Parlament gemäß s119A des Data Protection Act 2018 am 2. Februar 2022 vorgelegt wurde, in der Fassung, die gemäß Abschnitt 18 des Gesetzes über den Datenschutz (Data Protection Act 2018) überarbeitet werden kann und hier verfügbar ist [4].

"**EU-Standardvertragsklauseln 2021**" bezeichnet die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der DSGVO, die von der Europäischen Kommission im Rahmen des Durchführungsbeschlusses (EU) 2021/914 der Kommission angenommen wurden und hier abrufbar sind [3].

"**Geschützter Bereich**" bedeutet:

i. Im Falle von personenbezogenen Daten von EU-Kunden die Mitgliedstaaten der Europäischen Union und des Europäischen Wirtschaftsraums sowie alle Länder, Gebiete, Sektoren oder internationalen Organisationen, die einen Angemessenheitsbeschluss gemäß Artikel 45 DSGVO erhalten haben;

ii. Im Falle von personenbezogenen Daten von Kunden aus dem Vereinigten Königreich: das Vereinigte Königreich und alle Länder, Gebiete, Sektoren oder internationalen Organisationen, die eine Angemessenheitsentscheidung gemäß den britischen Angemessenheitsvorschriften erhalten haben;

iii. Im Falle von personenbezogenen Daten von Schweizer Kunden jedes Land, jedes Gebiet, jeder Sektor und jede internationale Organisation, die nach Schweizer Recht als angemessen anerkannt sind;

iv. Jedes andere Land, Territorium, jeder Sektor oder jede internationale Organisation, das/die nach den Gesetzen einer solchen Gerichtsbarkeit als angemessen anerkannt ist, wenn es sich um andere personenbezogene Kundendaten handelt, die aus einer Gerichtsbarkeit übermittelt werden, die einen ähnlichen Schutz bietet wie die personenbezogenen Kundendaten der EU, des Vereinigten Königreichs oder der Schweiz;

"**Personenbezogene Kundendaten aus der EU**" bezeichnet die Verarbeitung personenbezogener Kundendaten, auf die Datenschutzgesetze der Europäischen Union oder eines Mitgliedstaats der Europäischen Union oder des Europäischen Wirtschaftsraums vor ihrer Verarbeitung durch Iron Mountain anwendbar waren;

"**Personenbezogene Kundendaten aus der Schweiz**" bezeichnet die Verarbeitung personenbezogener Kundendaten, auf die vor der Verarbeitung durch Iron Mountain die Datenschutzgesetze der Schweiz anwendbar waren;

"**Persönliche Daten von britischen Kunden**" bezeichnet die Verarbeitung personenbezogener Kundendaten, auf die Datenschutzgesetze des Vereinigten Königreichs vor ihrer Verarbeitung durch Iron Mountain anwendbar waren;

"**Standardvertragsklauseln**" bedeutet insgesamt 2021 EU-Standardvertragsklauseln und 2022 UK Addendum.

2. VERSCHIEDENES

2.1 Dieser Anhang 3 enthält die folgenden Abschnitte: (i) Teil A - Übermittlung personenbezogener Daten von Kunden aus der EU; (ii) Teil B - Übermittlung personenbezogener Daten von Kunden aus der Schweiz; und (iii) Teil C - Übermittlung personenbezogener Daten von Kunden aus dem Vereinigten Königreich, die jeweils für die Übermittlung personenbezogener Daten von Kunden durch Iron Mountain in Verbindung mit seinen Dienstleistungen gelten.

2.2 Iron Mountain und seine verbundenen Unternehmen gelten als "Datenimporteure", und der Kunde und seine verbundenen Unternehmen gelten als "Datenexporteure".

2.3 Die Unterschrift und das Datum der Vereinbarung gelten als alle erforderlichen Unterschriften und Daten für die Standardvertragsklauseln.

---

[3] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

[4] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

2.4 Wenn die Parteien personenbezogene Daten von Kunden aus der EU, dem Vereinigten Königreich oder der Schweiz außerhalb des geschützten Bereichs übermitteln und eine einschlägige Entscheidung der Europäischen Kommission oder eine andere gültige Angemessenheitsmethode gemäß den geltenden Datenschutzvorschriften, auf die sich Iron Mountain bei der Datenübermittlung gestützt hat, für ungültig befunden wird, oder wenn eine Aufsichtsbehörde die Aussetzung der Übermittlung personenbezogener Daten gemäß einer solchen Entscheidung verlangt, müssen die Parteien zusammenarbeiten und eine solche Aussetzung erleichtern. Die Vertragsparteien sind sich ferner darüber einig, dass die in diesem Anhang 3 genannten angemessenen Schutzmaßnahmen zur Erleichterung internationaler Übertragungen nicht ausschließlich sind und dass die Vertragsparteien zusätzliche Übertragungsmechanismen, wie den EU-US-Übertragungsmechanismus, anwenden können. Datenschutz-Rahmen.

TEIL A - ÜBERMITTLUNG VON PERSONENBEZOGENEN DATEN VON EU-KUNDEN

Wenn und soweit der Kunde oder seine verbundenen Unternehmen personenbezogene Daten des EU-Kunden außerhalb des geschützten Bereichs an Iron Mountain oder seine verbundenen Unternehmen in Verbindung mit den Dienstleistungen des Vertrags übermitteln, gilt dieser Teil A von Anhang 3, und die Parteien vereinbaren Folgendes:

1. **Auswahl der Standardvertragsklauseln.** Der Text aus MODUL ZWEI der EU-Standardvertragsklauseln 2021 gilt, wenn der Kunde oder eines seiner verbundenen Unternehmen ein für die Verarbeitung Verantwortlicher und Iron Mountain oder eines seiner verbundenen Unternehmen ein Auftragsverarbeiter ist; der Text aus MODUL DREI der EU-Standardvertragsklauseln 2021 gilt, wenn der Kunde oder eines seiner verbundenen Unternehmen ein Auftragsverarbeiter und Iron Mountain oder eines seiner verbundenen Unternehmen ein Unterauftragsverarbeiter ist. Die einschlägigen Bestimmungen der EU-Standardvertragsklauseln von 2021 werden durch Verweis in diese DPA aufgenommen und sind integraler Bestandteil der DPA. Andere Module oder Klauseln, die in den EU-Standardvertragsklauseln 2021 als fakultativ gekennzeichnet sind, sind nicht anwendbar. Die für die Zwecke der Anhänge zu den EU-Standardvertragsklauseln 2021 erforderlichen Informationen sind in Anhang 1 - Beschreibung der Verarbeitung/Übermittlung, Anhang 2 - Technische und organisatorische Maßnahmen und Klausel 6.2 der DSGVO - Liste der Unterauftragsverarbeiter - aufgeführt.

2. **Einsatz von Unterauftragsnehmern.** Für die Zwecke der Klausel 9 der EU-Standardvertragsklauseln 2021 gilt die Option 2 (Allgemeine schriftliche Genehmigung) für den Einsatz von Unterauftragsverarbeitern für die Erbringung der Dienstleistungen. Der Kunde erkennt an und erklärt sich damit einverstanden, dass Iron Mountain neue Unterauftragsverarbeiter über den in Klausel 6 dieser DPA vereinbarten Mechanismus beauftragen kann und dass die Frist für die Einreichung von Anträgen auf Änderungen bei Unterauftragsverarbeitern fünfzehn (15) Tage beträgt.

3. **Geltendes Recht und Wahl des Gerichtsstands.** Option 2: Für die Zwecke von Klausel 17 der EU-Standardvertragsklauseln von 2021 (Anwendbares Recht) gilt das Recht des EU-Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, soweit dieses Recht die Rechte Dritter zulässt. Für die Zwecke von Klausel 18 der EU-Standardvertragsklauseln 2021 (Wahl des Gerichtsstands) sind dies die Gerichte des EU-Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

4. **Bescheinigung über die Löschung.** Für die Zwecke der Klauseln 8.5 und 16(d) der EU-Standardvertragsklauseln 2021 stellt Iron Mountain dem Kunden nur auf schriftlichen Antrag eine Bescheinigung über die Löschung personenbezogener Daten aus.

5. **Verstöße gegen personenbezogene Daten.** Für die Zwecke von Klausel 8.6(c) der EU-Standardvertragsklauseln von 2021 sind Verletzungen des Schutzes personenbezogener Daten gemäß dem in Klausel 7 der DSGVO vereinbarten Verfahren zu behandeln.

6. **Audits.** Für die Zwecke von Klausel 8.9 der EU-Standardvertragsklauseln von 2021 werden die Prüfungen dieser Klauseln gemäß dem in der Vereinbarung vereinbarten Prüfungsmechanismus durchgeführt.

7. **Beschwerden.** Für die Zwecke von Klausel 11 der EU-Standardvertragsklauseln von 2021 informiert Iron Mountain den Kunden, wenn es eine Beschwerde von einer betroffenen Person in Bezug auf personenbezogene Daten des EU-Kunden erhält, und teilt dem Kunden die Beschwerde gemäß dem im Vertrag vereinbarten Verfahren mit.

8. **Aufsichtsbehörde.** Für die EU-Standardvertragsklauseln 2022 wird die jeweils zuständige Aufsichtsbehörde in Übereinstimmung mit Klausel 13 der EU-Standardvertragsklauseln bestimmt.

TEIL B - ÜBERMITTLUNG VON PERSONENBEZOGENEN DATEN VON SCHWEIZER KUNDEN

Wenn und soweit der Kunde oder seine verbundenen Unternehmen personenbezogene Daten des Schweizer Kunden außerhalb des geschützten Bereichs an Iron Mountain oder seine verbundenen Unternehmen in

Verbindung mit den Dienstleistungen von Iron Mountain im Rahmen des Vertrags übermitteln, gilt dieser Teil B von Anhang 3, und die Parteien vereinbaren Folgendes:

1. **Auswahl der Standardvertragsklauseln.** Die EU-Standardvertragsklauseln 2021 und die einschlägigen Bestimmungen in Teil A gelten, wenn der Kunde oder eines seiner verbundenen Unternehmen ein für die Verarbeitung Verantwortlicher und Iron Mountain oder eines seiner verbundenen Unternehmen ein Auftragsverarbeiter ist und/oder der Kunde oder eines seiner verbundenen Unternehmen ein Auftragsverarbeiter und Iron Mountain oder eines seiner verbundenen Unternehmen ein Unterauftragsverarbeiter ist, mit der Ausnahme, dass:

   a. Die Eidgenössische Datenschutz- und Öffentlichkeitskommission (EDÖB) ist die zuständige Aufsichtsbehörde im Sinne von Artikel 13 der EU-Standardvertragsklauseln 2021;

   b. ist das anwendbare Recht für vertragliche Ansprüche nach Klausel 17 der EU-Standardvertragsklauseln 2021 schweizerisches Recht und der Gerichtsstand für Klagen zwischen den Parteien nach Klausel 18 (b) sind die schweizerischen Gerichte.

2. Verweise auf die EU-DSGVO in den EU-Standardvertragsklauseln 2021 sind als Verweise auf das DSG zu verstehen.

3. Der Begriff "Mitgliedstaat" in den EU-Standardvertragsklauseln 2021 ist nicht so auszulegen, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäß Klausel 18 (c) der EU-Standardvertragsklauseln 2021 einzuklagen.

TEIL C - ÜBERMITTLUNG VON PERSONENBEZOGENEN DATEN BRITISCHER KUNDEN

Wenn und soweit der Kunde oder seine verbundenen Unternehmen personenbezogene Daten des Vereinigten Königreichs außerhalb des geschützten Bereichs an Iron Mountain oder seine verbundenen Unternehmen in Verbindung mit den Dienstleistungen von Iron Mountain im Rahmen des Vertrags übermitteln, gilt dieser Teil C von Anhang 3, und die Parteien vereinbaren Folgendes:

1. **Auswahl der Standardvertragsklauseln.** Die EU-Standardvertragsklauseln 2021, die einschlägigen Bestimmungen in Teil A und der britische Nachtrag 2022 finden Anwendung, wenn der Kunde oder eines seiner verbundenen Unternehmen ein für die Verarbeitung Verantwortlicher und Iron Mountain oder eines seiner verbundenen Unternehmen ein Auftragsverarbeiter ist, und/oder wenn der Kunde oder eines seiner verbundenen Unternehmen ein Auftragsverarbeiter und Iron Mountain oder eines seiner verbundenen Unternehmen ein Unterauftragsverarbeiter ist.

2. **Teil 1: Tabelle 1 - 3 des Zusatzes 2022 UK:** Informationen über die Parteien - Tabelle 1; Ausgewählte SCCs, Module und ausgewählte Klauseln; und Informationen zu den Anlagen, einschließlich Anhang 1A: Liste der Parteien, Anhang 1B: Beschreibung des Transfers und Anhang 1C: Technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit - Tabelle 3 - gelten durch Bezugnahme auf diesen Anhang 3, einschließlich Teil A. Tabelle 4 des britischen Addendums, als abgeschlossen: Der Kunde und Iron Mountain erkennen an und vereinbaren, dass der britische Zusatzvertrag von jeder Partei gekündigt werden kann.

3. **Teil 2:** Obligatorische Klauseln des VK-Zusatzes: Der Kunde und Iron Mountain erkennen die obligatorischen Klauseln des britischen Nachtrags an und stimmen diesen zu.

4. **Aufsichtsbehörde.** Als zuständige Aufsichtsbehörde fungiert das UK Information Commissioner's Office.

TEIL D - ÜBERMITTLUNG ANDERER PERSONENBEZOGENER DATEN VON KUNDEN

Wenn und soweit der Kunde oder seine verbundenen Unternehmen personenbezogene Kundendaten, die nicht unter TEIL A-C fallen, an Iron Mountain oder seine verbundenen Unternehmen in Verbindung mit den Dienstleistungen von Iron Mountain im Rahmen des Vertrags übermitteln, gilt Teil A von Anhang 3 in dem Umfang, der gemäß den geltenden Datenschutzgesetzen relevant und anwendbar ist. Andernfalls vereinbaren die Parteien in dem Maße, in dem Ersatz- oder zusätzliche angemessene Schutzmaßnahmen oder Übermittlungsmechanismen gemäß den Datenschutzgesetzen erforderlich sind, um personenbezogene Kundendaten in ein Land zu übermitteln, das aus Sicht des Datenexporteurs kein angemessenes Schutzniveau für personenbezogene Daten bietet, diese so schnell wie möglich umzusetzen und diese Umsetzungsanforderungen in einer Anlage zu dieser DPA zu dokumentieren.

ANHANG 4

HIPAA - Geschäftspartner Vereinbarung ("BAA")

Diese BAA ergänzt und ändert alle gegenwärtigen oder zukünftigen Vereinbarungen zwischen Iron Mountain und seinen verbundenen Unternehmen und dem Kunden und seinen verbundenen Unternehmen, in deren Rahmen Iron Mountain oder seine verbundenen Unternehmen bestimmte Dienstleistungen für den Kunden oder seine verbundenen Unternehmen erbringen, die es erforderlich machen, dass der Geschäftspartner PHI im Namen der abgedeckten Einrichtung verwendet und/oder offenlegt. Sofern in dieser BAA keine Änderungen vorgenommen werden, bleiben alle Bestimmungen und Bedingungen des Vertrags in vollem Umfang in Kraft und regeln die von Iron Mountain für den Kunden erbrachten Dienstleistungen.

Iron Mountain und der Kunde schließen dieses BAA ab, damit beide Parteien ihren jeweiligen Verpflichtungen nachkommen können, sobald diese in Kraft treten und für die Parteien gemäß den HIPAA-Regeln zum Datenschutz, zur Sicherheit und zur Meldung von Datenschutzverletzungen zusammen mit allen Durchführungsbestimmungen, einschließlich der als Teil der Omnibus-Regel umgesetzten Bestimmungen (zusammenfassend als "HIPAA-Regeln" bezeichnet), nach denen der Kunde und seine verbundenen Unternehmen ein "betroffenes Unternehmen" oder "Geschäftspartner" und Iron Mountain und seine verbundenen Unternehmen ein "Geschäftspartner" des Kunden sind, verbindlich werden. Alle Verweise auf den Geschäftspartner in dieser Vereinbarung gelten als Verweise auf Iron Mountain oder seine jeweilige Tochtergesellschaft.

1. DEFINITIONEN

Großgeschriebene Begriffe, die in dieser BAA verwendet, aber nicht definiert werden, haben dieselbe Bedeutung wie in den HIPAA-Regeln oder dem Abkommen, je nach Anwendbarkeit.

Der Begriff "**Breach Notification Rule**" bezieht sich auf die Vorschrift für die Meldung von Verstößen bei ungesicherten geschützten Gesundheitsinformationen in 45 CFR § 164 Subpart D.

"**Geschäftspartner**" bezieht sich auf die oben genannte Einrichtung, die geschützte Gesundheitsdaten im Rahmen der Erbringung von Dienstleistungen für Kunden erhält, verwaltet oder überträgt.

"**Geschützte Gesundheitsinformationen**" oder "**PHI**" haben dieselbe Bedeutung wie der Begriff "geschützte Gesundheitsinformationen" in 45 CFR §160.103 und beschränken sich auf die PHI, die vom Geschäftspartner im Namen des Kunden erstellt werden oder die er von oder im Namen des Kunden gemäß der Vereinbarung erhält.

Der Begriff "**HIPAA**" bezieht sich auf den Health Insurance Portability and Accountability Act von 1996.

Der Begriff "**HITECH Act**" bezieht sich auf die Bestimmungen des Health Information Technology for Economic and Clinical Health Act, die in den American Recovery and Reinvestment Act von 2009 aufgenommen wurden, sowie auf alle Durchführungsbestimmungen.

Der Begriff "**Privacy Rule**" bezieht sich auf die Standards for Privacy of Individually Identifiable Health Information in 45 CFR § 160 und § 164, Subparts A und E.

"**Sicherheitsvorschrift**" bezeichnet die Sicherheitsstandards für den Schutz elektronischer geschützter Gesundheitsdaten in 45 CFR §160 und §164, Unterabschnitte A und C.

2. VERPFLICHTUNGEN UND TÄTIGKEITEN DES GESCHÄFTSPARTNERS

2.1. Der Geschäftspartner verpflichtet sich, PHI nur so zu verwenden oder weiterzugeben, wie es dieses BAA erlaubt oder erfordert oder wie es gesetzlich vorgeschrieben ist.

2.2. Der Geschäftspartner erklärt sich damit einverstanden, angemessene Sicherheitsvorkehrungen zu treffen und gegebenenfalls Unterabschnitt C von 45 CFR §164 in Bezug auf elektronische PHI einzuhalten, um zu verhindern, dass PHI auf andere Weise als in diesem BAA oder der Vereinbarung vorgesehen verwendet oder weitergegeben werden; die Parteien erkennen jedoch an und vereinbaren, dass es in der Verantwortung des Kunden und nicht des Geschäftspartners liegt, die Anforderungen gemäß 45 CFR §164.312, um Verschlüsselungs- oder Entschlüsselungsmechanismen für elektronische PHI zu implementieren, die auf physischen Medien (z. B. Bändern) aufbewahrt werden, die der Kunde beim Business Associate lagert.

2.3. Der Geschäftspartner verpflichtet sich, dem Kunden unverzüglich jeden Sicherheitsvorfall, jeden Verstoß oder jede andere Verwendung oder Offenlegung von PHI zu melden, von der er Kenntnis erlangt und die nicht durch dieses BAA oder die Vereinbarung erlaubt oder erforderlich ist. Im Falle eines Verstoßes erfolgt eine solche Benachrichtigung in Übereinstimmung mit den HIPAA-Regeln, einschließlich und ohne Einschränkung gemäß 45 CFR 164.410, aber in keinem Fall mehr als drei (3) Werktage, nachdem der Geschäftspartner seine interne Untersuchung abgeschlossen und bestätigt hat, dass ein Verstoß stattgefunden hat, und wie dies von einem Geschäftspartner verlangt wird. Der Geschäftspartner wird angemessene Unterstützung und Kooperation bei der Untersuchung eines solchen Verstoßes leisten und die spezifischen Einlagen, die kompromittiert wurden, die Identität von unbefugten Dritten, die auf die PHI zugegriffen oder diese erhalten haben, falls bekannt, und alle Maßnahmen, die der Geschäftspartner ergriffen hat, um die Auswirkungen eines solchen Verstoßes zu mildern, dokumentieren.

2.4. Der Geschäftspartner muss in Übereinstimmung mit 45 CFR 164.502(e)(1)(ii) und 164.308(b)(2)

sicherstellen, dass jeder Geschäftspartner, der ein Unterauftragnehmer ist, der PHI im Namen des Geschäftspartners zum Zweck der Unterstützung bei der Erbringung von Dienstleistungen gemäß der Vereinbarung erstellt, empfängt, aufbewahrt oder übermittelt, denselben Einschränkungen, Bedingungen und Anforderungen zustimmt, die für den Geschäftspartner in Bezug auf solche PHI durch diese BAA gelten.

2.5. Wenn der Geschäftspartner PHI in einem designierten Datensatz in Bezug auf Einzelpersonen verwahrt und der Kunde dies verlangt, erklärt sich der Geschäftspartner bereit, dem Kunden Zugang zu diesen PHI zu gewähren, indem er diese PHI in Übereinstimmung mit den Bedingungen der Vereinbarung abruft und ausliefert, damit der Kunde einer Einzelperson antworten kann, um die Anforderungen von 45 CFR §164.524 zu erfüllen.

2.6. Der Geschäftspartner erklärt sich damit einverstanden, dass, wenn eine Änderung von PHI in einem designierten Datensatz, der sich in der Obhut des Geschäftspartners befindet, erforderlich ist, und wenn der Kunde den Geschäftspartner anweist, diese PHI in Übereinstimmung mit der Vereinbarung abzurufen, der Geschäftspartner diese Dienstleistung erbringt, damit der Kunde alle Änderungen an diesen PHI vornehmen kann, die entweder vom Kunden oder einer Einzelperson gemäß 45 CFR §164.526 verlangt werden.

2.7. Der Geschäftspartner verpflichtet sich, dem Kunden die Informationen zu dokumentieren und zur Verfügung zu stellen, die erforderlich sind, um eine Buchführung über die Offenlegung von PHI zu erstellen, vorausgesetzt, der Kunde hat dem Geschäftspartner ausreichende Informationen zur Verfügung gestellt, die es dem Geschäftspartner ermöglichen, festzustellen, welche Aufzeichnungen oder Daten, die der Geschäftspartner vom oder im Namen des Kunden erhalten hat, PHI enthalten. Die Dokumentation der Offenlegungen muss die Informationen enthalten, die der Kunde benötigt, um auf die Anfrage einer Person nach einer Buchführung über Offenlegungen von PHI gemäß 45 CFR §164.528 oder anderen Bestimmungen der HIPAA-Regeln zu antworten.

2.8. Sofern in der Vereinbarung nicht ausdrücklich etwas anderes vereinbart wurde, muss der Geschäftspartner den Kunden unverzüglich über alle Anfragen von Einzelpersonen nach Zugang, Kenntnis oder Berichtigung von PHI benachrichtigen, ohne auf solche Anfragen zu reagieren, und der Kunde ist für den Erhalt und die Beantwortung solcher Anfragen von Einzelpersonen verantwortlich.

2.9. Soweit der Business Associate eine oder mehrere der Verpflichtungen des Kunden gemäß Subpart E von 45 CFR §164 erfüllen soll, muss der Business Associate die Anforderungen von Subpart E einhalten, die für den Kunden bei der Erfüllung dieser Verpflichtung(en) gelten.

2.10. Der Geschäftspartner erklärt sich bereit, dem Sekretär seine internen Praktiken, Bücher und Aufzeichnungen zur Verfügung zu stellen, um die Einhaltung der HIPAA-Regeln zu überprüfen.

3. ERLAUBTE VERWENDUNGEN UND OFFENLEGUNGEN DURCH GESCHÄFTSPARTNER

3.1. Der Geschäftspartner darf PHI verwenden oder weitergeben, soweit dies zur Erbringung der in der Vereinbarung festgelegten Dienstleistungen erforderlich ist.

3.2. Der Geschäftspartner kann PHI verwenden oder weitergeben, wenn dies gesetzlich vorgeschrieben ist.

3.3. Der Geschäftspartner verpflichtet sich, angemessene Anstrengungen zu unternehmen, um PHI auf das Minimum zu beschränken, das zur Erreichung des beabsichtigten Zwecks der Nutzung, Offenlegung oder Anfrage erforderlich ist.

3.4. Der Geschäftspartner darf PHI nicht in einer Weise verwenden oder offenlegen, die gegen Subpart E von 45 CFR §164, wenn dies durch den Kunden geschieht.

3.5. Der Geschäftspartner darf PHI für die ordnungsgemäße Geschäftsführung und Verwaltung des Geschäftspartners oder zur Erfüllung der gesetzlichen Pflichten des Geschäftspartners offenlegen, sofern die Offenlegung gesetzlich vorgeschrieben ist oder der Geschäftspartner von der Person, der die Informationen offengelegt werden, angemessene Zusicherungen erhält, dass die Informationen vertraulich bleiben und nur wie gesetzlich vorgeschrieben oder für die Zwecke, für die sie der Person offengelegt wurden, verwendet oder weitergegeben werden, und die Person den Geschäftspartner über alle ihr bekannten Fälle informiert, in denen die Vertraulichkeit der Informationen verletzt wurde.

4. PFLICHTEN DES KUNDEN

4.1. Der Kunde darf den Geschäftspartner nicht anweisen, in einer Weise zu handeln, die nicht mit den HIPAA-Regeln übereinstimmt.

4.2. Der Kunde muss den Geschäftspartner über jede Einschränkung in seiner Mitteilung über die Datenschutzpraktiken des Kunden gemäß 45 CFR §164.520 informieren, soweit diese Einschränkung die Verwendung oder Offenlegung von PHI durch den Geschäftspartner beeinflussen kann.

4.3. Der Kunde muss den Geschäftspartner über alle Änderungen oder den Widerruf der Erlaubnis einer Person zur Verwendung oder Offenlegung ihrer PHI informieren, soweit diese Änderungen die Verwendung oder Offenlegung von PHI durch den Geschäftspartner beeinflussen können.

4.4. Der Kunde muss den Geschäftspartner schriftlich über jede Einschränkung der Verwendung oder Weitergabe von PHI informieren, der Kunde gemäß 45 CFR §164.522 zugestimmt hat, soweit diese Einschränkung die Verwendung oder Weitergabe von PHI durch den Geschäftspartner beeinflussen kann.

5. LAUFZEIT UND KÜNDIGUNG

5.1. Die Laufzeit dieses BAA beginnt am Tag des Inkrafttretens und endet automatisch, wenn entweder (i) die

Vereinbarung ausläuft oder (ii) alle PHI, die der Kunde dem Geschäftspartner zur Verfügung stellt, vernichtet oder an den Kunden zurückgegeben werden.

5.2. Sobald eine Partei von einer wesentlichen Verletzung der BAA durch die andere Partei Kenntnis erlangt, muss die nicht verletzende Partei der verletzenden Partei die Möglichkeit geben, die Verletzung zu beheben. Gelingt es der verletzenden Partei nicht, die Verletzung innerhalb von dreißig (30) Tagen nach Erhalt einer schriftlichen Mitteilung der nicht verletzenden Partei, in der die Einzelheiten der wesentlichen Verletzung dargelegt sind, zu beheben, hat die nicht verletzende Partei das Recht, dieses BAA und die Vereinbarung gemäß den Bedingungen der Vereinbarung zu kündigen, oder, falls eine Kündigung nicht möglich ist, das Problem dem Sekretär oder einer anderen zuständigen Behörde zu melden.

5.3. Wirkung der Beendigung:

5.3.1.1. Mit Ausnahme der Bestimmungen in 5.3.2 ist der Geschäftspartner bei Beendigung dieses BAA aus irgendeinem Grund verpflichtet, alle vom Kunden erhaltenen PHI in Übereinstimmung mit der Vereinbarung zurückzugeben oder zu vernichten. Diese Bestimmung gilt für PHI, die sich im Besitz von Unterauftragnehmern oder Vertretern des Geschäftspartners befinden. Der Geschäftspartner darf keine Kopien der PHI aufbewahren.

5.3.1.2. Wenn der Geschäftspartner feststellt, dass die Rückgabe oder Vernichtung der PHI unmöglich ist, muss der Geschäftspartner den Kunden über die Bedingungen informieren, die eine Rückgabe oder Vernichtung unmöglich machen. Nach Benachrichtigung des Kunden wird der Geschäftspartner den Schutz dieses BAA auf solche PHI ausdehnen und weitere Verwendungen und Offenlegungen solcher PHI auf die Zwecke beschränken, die eine Rückgabe oder Vernichtung unpraktisch machen, solange der Geschäftspartner solche PHI in Übereinstimmung mit den Bedingungen der Vereinbarung aufbewahrt.

6. VERSCHIEDENES

6.1. Entschädigung. Der Geschäftspartner erklärt sich damit einverstanden, den Kunden von und gegen jegliche Geldbußen oder Strafen freizustellen, die dem Kunden infolge eines vom Secretary eingeleiteten Vollstreckungsverfahrens oder einer vom Generalstaatsanwalt eines Bundesstaates gegen den Kunden angestrengten Zivilklage auferlegt werden, wobei dieses Verfahren oder diese Klage direkt und ausschließlich aus einer Handlung oder Unterlassung des Geschäftspartners resultiert, die entweder eine Verletzung der HIPAA-Regeln oder eine wesentliche Verletzung dieses BAA darstellt ("Anspruch"). Der Geschäftspartner ist nicht verpflichtet, den Kunden für einen Teil solcher Bußgelder oder Strafen zu entschädigen, die sich aus (i) einem Verstoß des Kunden gegen die HIPAA-Regeln oder dieses BAA oder (ii) fahrlässigen oder vorsätzlichen Handlungen oder Unterlassungen des Kunden ergeben. Die vorstehende Freistellungsverpflichtung ist ausdrücklich an die Bedingung geknüpft, dass der Kunde Business Associate das Recht einräumt, nach eigenem Ermessen und auf eigene Kosten mit einem Anwalt seiner Wahl die Verteidigung gegen einen solchen Anspruch zu kontrollieren oder sich daran zu beteiligen, jedoch unter der Voraussetzung, dass, sofern ein solcher Anspruch Teil eines größeren Verfahrens oder einer größeren Klage ist, das Recht von Business Associate zur Kontrolle oder Beteiligung auf den Anspruch und nicht auf das größere Verfahren oder die größere Klage beschränkt ist. Macht der Geschäftspartner von seiner Option Gebrauch, die Verteidigung zu kontrollieren, dann (i) wird der Geschäftspartner keine Ansprüche begleichen, die ein Eingeständnis eines Verschuldens seitens des Kunden erfordern, ohne dessen vorherige schriftliche Zustimmung, (ii) hat der Kunde das Recht, sich auf eigene Kosten an der Klage oder dem Prozess zu beteiligen und (iii) wird der Kunde mit dem Geschäftspartner zusammenarbeiten, wie es angemessenerweise verlangt werden kann. Das Vorstehende legt das einzige und ausschließliche Rechtsmittel des Kunden und die einzige Haftung des Geschäftspartners für jegliche Verluste, Schäden, Kosten oder Haftungen des Kunden für Ansprüche im Zusammenhang mit diesem BAA fest.

6.2. Unterlassungsklagen. Der Geschäftspartner erkennt an, dass jede unbefugte Nutzung oder Weitergabe von PHI durch den Geschäftspartner dem Kunden einen nicht wiedergutzumachenden Schaden zufügen kann, für den der Kunde eine einstweilige Verfügung oder einen anderen gerechten Rechtsbehelf beantragen kann, wenn er sich dafür entscheidet.

6.3. Regulatorische Referenzen. Ein Verweis in dieser BAA auf einen Abschnitt der HIPAA-Regeln bezeichnet den Abschnitt des HIPAA, die Privacy Rule, die Security Rule, den HITECH ACT oder die endgültigen Omnibus-Regeln in ihrer geänderten und gültigen Fassung, für die eine Einhaltung erforderlich ist.

6.4. Abänderung. Die Parteien vereinbaren, nach Treu und Glauben über jede Änderung dieses BAA zu verhandeln, die von Zeit zu Zeit erforderlich ist, damit der Kunde oder der Geschäftspartner die Anforderungen der HIPAA-Regeln erfüllen kann. Wenn die Parteien nicht in der Lage sind, innerhalb von sechzig (60) Tagen nach Erhalt eines solchen schriftlichen Antrags des Kunden an den Geschäftspartner eine gegenseitige Einigung über die Bedingungen einer solchen Änderung zu erzielen, kann jede Partei dieses BAA und die Vereinbarung durch eine schriftliche Mitteilung an die andere Partei mit einer Frist von mindestens dreißig (30) Tagen kündigen.

6.5. Keine dritten Begünstigten. Nichts in dieser BAA ist beabsichtigt oder impliziert, um Rechte, Rechtsmittel, Verpflichtungen oder Haftungen auf andere Personen als den Kunden, den Geschäftspartner und ihre jeweiligen Nachfolger oder Zessionare zu übertragen, und nichts in dieser BAA soll diese übertragen.

6.6. Unabhängiger Auftragnehmer. Der Geschäftspartner, einschließlich seiner Direktoren, leitenden Angestellten, Mitarbeiter und Beauftragten, ist ein unabhängiger Auftragnehmer und kein Vertreter des Kunden (im Sinne des bundesstaatlichen Common Law of Agency) oder ein Mitglied seiner Belegschaft. Ohne die Allgemeingültigkeit des Vorstehenden einzuschränken, hat der Kunde kein Recht, das Verhalten

des Geschäftspartners bei der Erbringung der Dienstleistungen zu kontrollieren, zu lenken oder anderweitig zu beeinflussen, es sei denn durch die Durchsetzung dieses BAA oder der Vereinbarung oder durch deren gegenseitige Änderung.

6.7. Vorrang; gesamtes Abkommen. Jede Unklarheit in diesem BAA muss geklärt werden, damit die Parteien die HIPAA-Vorschriften einhalten können. Diese BAA stellt die gesamte Vereinbarung der Parteien in Bezug auf den Gegenstand dieser BAA dar und ersetzt alle früheren Mitteilungen, Zusicherungen, Vereinbarungen und Absprachen im Zusammenhang mit den HIPAA-Regeln, einschließlich aller früheren Geschäftspartnervereinbarungen zwischen den Parteien.