**ERGÄNZUNG ZUR WEITERGABE VON DATEN (UNTERNEHMENSDATEN)**

**Revisionsdatum: 12. März 2024**

Für die Zwecke dieses Nachtrats zur Weitergabe von Daten („Data Sharing Addendum, DSA“) wird das Unternehmen oder die Tochtergesellschaft von Merck Sharp & Dohme LLC, das bzw. die die Vereinbarung oder eine andere Form der Vereinbarung, die auf dieses DSA verweist (die „Vereinbarung“), ausführt, als „Unternehmen“ bezeichnet und alle anderen Parteien einer solchen Vereinbarung werden gemeinsam als „Anbieter“ bezeichnet. Das Unternehmen und der Anbieter werden jeweils als „Partei“ und gemeinsam als „die Parteien“ bezeichnet.

Hintergrund

1. Die Parteien haben die Vereinbarung geschlossen und können zusammen mit der Vereinbarung einen oder mehrere Kauf- oder Arbeitsaufträge, Projektvereinbarungen, Anhänge von Projektplänen, Leistungsbeschreibungen, Arbeitsaufträge oder andere Dienstleistungsbedingungen (jeweils eine „Leistungsbeschreibung“) abschließen, die die darin vorgesehenen Dienstleistungen (den „Zweck der Datenweitergabe“) regeln.
2. Die Parteien beabsichtigen, die Bedingungen der Vereinbarung zu ergänzen, um sicherzustellen, dass die gesamte Weitergabe personenbezogener Daten im Zusammenhang mit der Vereinbarung in Übereinstimmung mit dem Datenschutzrecht erfolgt, und um die Rolle des Anbieters als unabhängiger Verantwortlicher dieser Daten festzulegen.

Die Parteien vereinbaren:

1. *Aktivitäten zur Weitergabe von Daten*. In Bezug auf personenbezogene Daten, die im Zusammenhang mit der Vereinbarung verarbeitet werden, sind Gegenstand, Art, Zweck und Dauer der Weitergabe, die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten im Anhang der Vereinbarung mit dem Titel „Datenverarbeitung im Einzelnen“ aufgeführt.
2. *Anwendbarkeit*. Die Bestimmungen dieses DSA gelten für jeden Arbeitsauftrag im Rahmen der Vereinbarung, sofern in diesem Arbeitsauftrag nichts anderes festgelegt ist.
3. *Pflichten des Anbieters*. Bei der Verarbeitung personenbezogener Daten im Zusammenhang mit der Vereinbarung
	1. muss der Anbieter die Datenschutzgesetze und seine Verpflichtungen aus dieser DSA einhalten. Kann der Anbieter diesen Verpflichtungen nicht nachkommen, muss er das Unternehmen unverzüglich benachrichtigen und alle angemessenen und geeigneten Maßnahmen ergreifen, die das Unternehmen für notwendig hält, um die Nichteinhaltung zu beheben.
	2. darf der Anbieter personenbezogene Daten nur wie in dieser DSA und der Vereinbarung angegeben verarbeiten, es sei denn,
		1. der Anbieter die vorherige Einwilligung der betroffenen Person eingeholt hat;
		2. dies ist für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen im Rahmen bestimmter Verwaltungs-, Aufsichts- oder Gerichtsverfahren erforderlich;
		3. es ist notwendig, die lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; oder
		4. der Anbieter ist durch geltendes Recht zu etwas anderem verpflichtet. In diesem Fall informiert der Anbieter das Unternehmen über diese gesetzliche Verpflichtung, es sei denn, dies ist durch geltendes Recht untersagt, und er bemüht sich nach besten Kräften, Art und Umfang der erforderlichen Offenlegung zu begrenzen, und legt nur das Minimum an personenbezogenen Daten offen, das zur Einhaltung des geltenden Rechts erforderlich ist.
	3. darf der Anbieter personenbezogene Daten nicht an Dritte weitergeben oder übertragen, ohne dass diese Dritten eine schriftliche Vereinbarung treffen, deren Bedingungen den Schutz personenbezogener Daten mindestens ebenso gut gewährleisten wie die in dieser DSA und der Vereinbarung dargelegten Verpflichtungen.
	4. ist der Anbieter nicht berechtigt, persönliche Daten zu verkaufen, weiterzugeben, zu speichern, zu verwenden oder offenzulegen, es sei denn, dies ist in der Vereinbarung festgelegt oder anderweitig im Rahmen dieser DSA genehmigt.
	5. haftet der Anbieter in vollem Umfang für alle Handlungen oder Unterlassungen seiner Mitarbeitenden, verbundenen Unternehmen, Vertreter, Nachunternehmer oder anderen Beauftragten.
	6. implementiert und pflegt der Anbieter angemessene und geeignete schriftliche Informationssicherheits- und Datenschutzprogramme, die physische, technische und organisatorische Maßnahmen umfassen, die der Art der im Zusammenhang mit der Vereinbarung verarbeiteten personenbezogenen Daten entsprechen, die die guten Branchenverfahren (oder einen höheren Standard, wie er in Anhang 1 gefordert wird) erfüllen oder übertreffen und die einen angemessenen Schutz vor einer Verletzung des Schutzes personenbezogener Daten bieten, einschließlich der Schulung aller für die Verarbeitung personenbezogener Daten verantwortlichen Mitarbeiter in einer Weise, die ausreicht, um die Anforderungen dieser DSA zu erfüllen, sowie der in Anhang 1 beschriebenen Maßnahmen und, soweit in Anhang 1 nicht anderweitig geregelt und bei Bedarf:
		1. die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten;
		2. die Möglichkeit, die ständige Vertraulichkeit, Integrität, Verfügbarkeit und Stabilität der Verarbeitungssysteme und Verarbeitungsdienste zu gewährleisten;
		3. die Möglichkeit, bei technischen Zwischenfällen die Verfügbarkeit und den Zugriff auf personenbezogene Daten rasch wieder herzustellen;
		4. ein Verfahren für die regelmäßige Prüfung, Bewertung und Evaluierung der Effektivität technischer und organisatorischer Maßnahmen zur Gewährleistung der Verarbeitungssicherheit; und
		5. die Möglichkeit, innerhalb von 72 Stunden nach der Erkennung zu bestätigen, ob ein Ereignis eine Verletzung des Schutzes personenbezogener Daten darstellt.
	7. ist der Anbieter verpflichtet, im Falle einer tatsächlichen oder vernünftigerweise vermuteten Verletzung des Schutzes personenbezogener Daten, die sich im Gewahrsam oder unter der Kontrolle des Anbieters befinden oder die auf Handlungen oder Unterlassungen des Anbieters zurückzuführen sind (eine „Verletzung des Schutzes personenbezogener Daten durch den Anbieter“), Folgendes zu tun:
		1. das Unternehmen unverzüglich benachrichtigen (und in jedem Fall innerhalb von 24 Stunden nach Kenntniserlangung einer Verletzung des Schutzes personenbezogener Daten durch den Anbieter);
		2. eine angemessene Untersuchung durchführen und alle erforderlichen Abhilfemaßnahmen ergreifen, um eine solche Verletzung des Schutzes personenbezogener Daten durch den Anbieter in einer für das Unternehmen zufriedenstellenden Weise zu beheben und eine Wiederholung zu verhindern;
		3. dem Unternehmen unverzüglich alle Informationen zur Verfügung stellen, die das Unternehmen für notwendig erachtet, um die Datenschutzgesetze einzuhalten, auch in Bezug auf die Führung von Aufzeichnungen und die Berichterstattung, sowie alle anderen Informationen, die das Unternehmen in Bezug auf eine Verletzung des Schutzes personenbezogener Daten durch den Anbieter vernünftigerweise anfordert;
		4. alle betroffenen Personen benachrichtigen, deren personenbezogene Daten möglicherweise betroffen sind, mit den gemäß Datenschutzgesetz erforderlichen Inhalten; und
		5. die alleinige Verantwortung für die Kosten und Ausgaben einer Partei für eine solche Benachrichtigung der betroffenen Personen tragen, unabhängig davon, ob die Benachrichtigung durch den Anbieter oder das Unternehmen erfolgt ist.
	8. muss der Anbieter unverzüglich das Unternehmen verständigen, und jedenfalls innerhalb von 24 Stunden, in Bezug auf:
		1. jede/n/s Beschwerde, Anfrage, Antrag oder Anliegen einer zuständigen Datenschutz- oder sonstigen Aufsichtsbehörde in Bezug auf personenbezogene Daten, die der Anbieter im Zusammenhang mit der Vereinbarung verarbeitet und
		2. jede/n/s Beschwerde, Anfrage, Antrag oder Anliegen einer betroffenen Person in Bezug auf personenbezogene Daten im Zusammenhang mit der Vereinbarung, einschließlich der Ausübung von Rechten nach dem Datenschutzgesetz oder der Datenschutzrichtlinie des Unternehmens oder des Anbieters, wie z. B. das Recht auf Zugang (einschließlich der Anforderung von Informationen über die Verarbeitung ihrer personenbezogenen Daten), Berichtigung, Ergänzung, Korrektur, Freigabe, Löschung oder Einstellung der Verarbeitung ihrer personenbezogenen Daten.
	9. muss der Anbieter alle vom Unternehmen geforderten angemessenen und geeigneten Maßnahmen ergreifen, die erforderlich sind, damit der Anbieter und das Unternehmen ihren jeweiligen Verpflichtungen aus dem Datenschutzgesetz und dieser DSA nachkommen können.
	10. darf der Anbieter personenbezogene Daten nicht länger aufbewahren, als es für die Erfüllung des Zwecks der Weitergabe von Daten erforderlich ist, sofern das geltende Recht nichts anderes vorschreibt.
	11. muss der Anbieter die Richtigkeit und Integrität der vom Unternehmen weitergegebenen personenbezogenen Daten in der Form pflegen, in der er diese personenbezogenen Daten erhalten oder erfasst hat.
	12. muss der Anbieter alle Aufzeichnungen bewahren, die für den Nachweis erforderlich sind, dass personenbezogene Daten ausschließlich in Übereinstimmung mit den einschlägigen Hinweisen, Einverständniserklärungen und Rechten und gemäß dieser DSA verarbeitet wurden, damit sowohl das Unternehmen als auch der Anbieter die Datenschutzbestimmungen einhalten kann.
	13. Soweit der Anbieter personenbezogene Daten von Betroffenen aus einem Land oder einer Region verarbeitet, in dem/der Beschränkungen für die grenzüberschreitende Übermittlung personenbezogener Daten bestehen, darf der Anbieter dies nur unter Einhaltung der Datenschutzgesetze tun, wozu unter anderem der Abschluss von Standardvertragsklauseln oder ähnlichen Mechanismen zum Schutz der Übermittlung personenbezogener Daten gehören kann.
	14. Mit Ausnahme von Änderungen, die im Einklang mit einem höheren Industriestandard oder dem Datenschutzgesetz vorgenommen werden, muss der Anbieter die Datenschutz- und Datensicherheits-praktiken, die er dem Unternehmen in Verbindung mit einer Due-Diligence-Prüfung, die das Unternehmen zuletzt im Zusammenhang mit der Vereinbarung durchgeführt hat, offengelegt hat, beibehalten und konsequent anwenden; vorausgesetzt, dass der Anbieter die Standards dieser Praktiken nicht dadurch herabsetzen darf, dass er später Datenschutz- und Datensicherheitspraktiken offenlegt, die eine Verschlechterung der zuvor offengelegten Praktiken darstellen würden. Der Anbieter sichert zu und gewährleistet, dass alle von ihm im Rahmen einer solchen Due Diligence gemachten Angaben wahrheitsgemäß, genau und vollständig sind und dass ein bevollmächtigter Vertreter des Anbieters diese Due Diligence durchgeführt hat. Der Anbieter muss dem Unternehmen unverzüglich alle wesentlichen Änderungen der Datenschutz- und Datensicherheitspraktiken des Anbieters mitteilen.
	15. Der Anbieter ernennt, sofern dies durch das Datenschutzgesetz vorgeschrieben ist, eine Person, die mit dem Schutz personenbezogener Daten betraut ist, und teilt dem Unternehmen den Namen und die Kontaktdaten dieser Person mit.
	16. Der Anbieter nimmt zur Kenntnis und ist damit einverstanden, dass die Unterzeichnung dieser DSA die Bestätigung darstellt, dass er die in dieser DSA dargelegten Einschränkungen versteht und diese einhalten wird.
4. *Schadloshaltung*. Ohne die Rechte oder Ansprüche des Unternehmens oder die Verpflichtungen des Anbieters im Rahmen der Vereinbarung oder anderweitig einzuschränken, vereinbaren die Parteien, dass der Anbieter das Unternehmen und seine verbundenen Unternehmen sowie deren leitenden Angestellten, Direktoren, Mitarbeiter, Auftragnehmer, Zeitarbeiter, Nachunternehmer, Vertreter und andere Beauftragten (jeweils eine „entschädigte Partei“) für alle Verluste, Schäden, Bußgelder, Kosten oder Auslagen (einschließlich Anwaltskosten und Auslagen) entschädigt, die der entschädigten Partei aufgrund einer Verletzung des Schutzes personenbezogener Daten durch den Anbieter in Bezug auf die vom Anbieter im Zusammenhang mit der Vereinbarung verarbeiteten personenbezogenen Daten entstehen. Jegliche Haftung im Rahmen dieses Abschnitts unterliegt den geltenden Haftungsbeschränkungen oder -ausschlüssen der Vereinbarung, es sei denn, eine solche Haftung ist das Ergebnis einer Fahrlässigkeit oder eines vorsätzlichen Fehlverhaltens des Anbieters; in diesem Fall gelten keine Beschränkungen oder Ausschlüsse.
5. *Definitionen*
	1. „Datenschutzgesetz“ bezeichnet alle anwendbaren Gesetze zum Datenschutz, zur Datensicherheit oder zum Schutz der Privatsphäre, einschließlich der EU-Datenschutzgrundverordnung und aller damit verbundenen nationalen Umsetzungsgesetze, des Health Insurance Portability and Accountability Act, des California Privacy Rights Act und aller anderen nationalen, staatlichen, bundesweiten, landesweiten oder regionalen Gesetze zum Datenschutz, zur Datensicherheit oder zum Schutz der Privatsphäre.
	2. „Personenbezogene Daten“ bezeichnet alle Daten im Zusammenhang mit der Vereinbarung, die sich auf eine identifizierte oder identifizierbare Person beziehen, einschließlich Daten, die eine Person identifizieren oder die verwendet werden könnten, um eine Person zu identifizieren, zu lokalisieren, zu verfolgen oder zu kontaktieren. Personenbezogene Daten umfassen sowohl direkt identifizierbare Informationen, wie z. B. Name, Identifikationsnummer oder eindeutige Berufsbezeichnung, als auch indirekt identifizierbare Informationen, wie z. B. Geburtsdatum, eindeutige Kennung eines mobilen oder tragbaren Geräts, Informationen, die zur Identifizierung eines Haushalts verwendet werden könnten, Telefonnummern, verschlüsselte Daten, Online-Kennungen, wie z. B. IP-Adressen, oder persönliche Aktivitäten, Verhaltensweisen oder Vorlieben, und umfassen alle Daten, die im Sinne des Datenschutzgesetzes „personenbezogene Daten“ darstellen.
	3. „Verarbeitung“ bedeutet die Durchführung von Vorgängen oder einer Reihe von Vorgängen an personenbezogenen Daten oder einem Satz personenbezogener Daten, sei es durch automatisierte Mittel, wie z. B. Erhebung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Zugriff, Anpassung oder Veränderung, Abruf, Abfrage, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder sonstige Bereitstellung, Auswertung, Analyse, Berichterstattung, Weitergabe, Zuordnung oder Verknüpfung, Einschränkung, Löschung oder Vernichtung.
	4. „Verletzung des Schutzes personenbezogener Daten“ bezeichnet eine versehentliche oder unrechtmäßige Zerstörung, einen Verlust, eine Änderung, eine unbefugte Offenlegung oder einen unbefugten Zugriff auf personenbezogene Daten, die übermittelt, gespeichert oder anderweitig verarbeitet werden.
	5. „Standardvertragsklauseln“ bezeichnet die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, die nach Einschätzung der Europäischen Kommission kein angemessenes Schutzniveau für personenbezogene Daten bieten, gemäß der von der Europäischen Kommission am 4. Juni 2021 veröffentlichten Fassung, die von Zeit zu Zeit aktualisiert werden kann.
	6. Falls diese Definitionen den Geltungsbereich verwandter Definitionen des Datenschutzgesetzes einschränken oder reduzieren, wird die Definition so erweitert, dass sie mit der Definition des betreffenden Datenschutzgesetzes übereinstimmt.
	7. In Ermangelung einer Definition in diesem Abschnitt ist ein Begriff in einer Weise auszulegen, die mit allen anwendbaren Datenschutzgesetzen vereinbar ist.
6. *Auslegung*.
	1. Definierte Begriffe, die in dieser DSA verwendet werden, aber hier nicht definiert sind, haben die an anderer Stelle in dieser Vereinbarung festgelegte Bedeutung.
	2. Die Wörter „umfassen“ und „einschließlich“ sind so aufzufassen, dass sie „einschließlich ohne Einschränkung“ bedeuten.
	3. Bei der Erfüllung ihrer Verpflichtungen aus dem Dienstleistungsvertrag und dieser DSA erkennen die Parteien an, dass die Unternehmensrichtlinie von MSD und seinen verbundenen Unternehmen verlangt, dass die Geschäfte von MSD im Einklang mit dem Wortlaut und dem Geist der geltenden Datenschutzgesetze, einschließlich der EU-Datenschutz-Grundverordnung, geführt werden. Für den Fall, dass beide Parteien nicht denselben Datenschutzgesetzen unterliegen, wird erwartet, dass beide Parteien alle in diesen Gesetzen enthaltenen relevanten Datenschutzstandards einhalten.
	4. In Verbindung mit dem Zweck der Weitergabe von Daten im Rahmen der Vereinbarung kann der Anbieter personenbezogene Daten eines oder mehrerer verbundener Unternehmen des Unternehmens verarbeiten. In diesem Fall gilt jedes dieser verbundenen Unternehmen des Unternehmens als „für die Verarbeitung Verantwortlicher“ personenbezogener Daten und als Drittbegünstigter dieser DSA und ist berechtigt, sich auf alle Rechte und Schutzmaßnahmen zu berufen, die dem Unternehmen im Rahmen dieser DSA gewährt werden, unabhängig davon, ob dieses verbundene Unternehmen als Partei der Vereinbarung oder dieser DSA genannt ist.
	5. Diese DSA wird hiermit in die Vereinbarung aufgenommen und bildet einen Teil davon.
	6. Im Falle und im Ausmaß von Widersprüchen zwischen den Bedingungen der Vereinbarung und dieser DSA haben die Bedingungen dieser DSA Vorrang, es sei denn, die Bedingungen der Vereinbarung schützen die im Zusammenhang mit der Vereinbarung verarbeiteten personenbezogenen Daten besser; in diesem Fall haben die den besseren Schutz bietenden Bedingungen dieser Vereinbarung Vorrang.
	7. Im Falle eines Widerspruchs zwischen den Bestimmungen dieser DSA und den Standardvertragsklauseln sind die Bestimmungen der Standardvertragsklauseln maßgebend.
	8. Sofern hierin nicht ausdrücklich geändert, bleiben die Bedingungen der Vereinbarung in vollem Umfang in Kraft und wirksam.
	9. Wenn diese DSA in englischer und in einer anderen Sprache verfasst wurde, ist im Falle von Unterschieden zwischen dem englischen und dem anderssprachigen Text die englische Version maßgebend.
	10. Überschriften in dieser DSA dienen ausschließlich der Übersichtlichkeit und stellen keinen Bestandteil dieser DSA dar und haben keinen Einfluss auf die Bedeutung oder Auslegung dieser DSA.
	11. Anhänge und Anlagen zu dieser DSA gelten im gleichen Maße als Bestandteil dieser DSA, als wären sie wörtlich in dieser DSA aufgeführt.
	12. Die Bestimmungen dieser DSA sind trennbar. Sollte ein Satz, eine Klausel oder eine Bestimmung vollständig oder teilweise ungültig oder nicht durchsetzbar sein, betrifft diese Ungültigkeit oder Nichtdurchsetzbarkeit ausschließlich diesen Satz, diese Klausel oder diese Bestimmung und bleiben die übrigen Bestimmungen dieser DSA uneingeschränkt rechtswirksam.
	13. Diese DSA regelt die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Zweck der Weitergabe von Daten und ergänzt die Bedingungen der für den Zweck der Weitergabe von Daten geltenden Vereinbarung, es sei denn, das Unternehmen und der Anbieter haben eine andere DSA abgeschlossen, die für bestimmte Zwecke der Weitergabe von Daten gilt.
	14. Diese DSA kann in einer beliebigen Anzahl Ausfertigungen geschlossen werden, die alle zusammen eine einzige und dieselbe Vereinbarung darstellen. Jede Partei kann diese DSA durch Unterzeichnung einer Ausfertigung eingehen.
	15. Diese DSA stellt die gesamte Vereinbarung zwischen den Parteien in Bezug auf den Gegenstand dieser DSA dar und ersetzt (soweit gesetzlich zulässig) alle früheren Zusicherungen oder mündlichen oder schriftlichen Vereinbarungen zwischen den Parteien in Bezug auf diesen Gegenstand, vorausgesetzt, nichts in dieser DSA und keine der Parteien versucht, eine Haftung für betrügerische Angaben auszuschließen.
	16. Die Bestimmungen der Vereinbarung bezüglich des geltenden Rechts und des Gerichtsstands finden auf diese DSA Anwendung.
7. *Beschränkungen für Updates*.
	1. Wenn die Parteien die Vereinbarung erneuern, ändern, eine neue Leistungsbeschreibung unter der Vereinbarung ausstellen oder die Vereinbarung oder eine Leistungsbeschreibung unter der Vereinbarung in irgendeiner Weise ändern (ein "auslösendes Ereignis"), wird das neueste Dokument unter " Data Sharing Addendum (Company Data)" an der Stelle <https://www.msdprivacy.com/privacyterms/> die Bedingungen dieses DSA ersetzen und außer Kraft setzen, bis das nächste auslösende Ereignis eintritt, es sei denn, es wird innerhalb von 30 Tagen nach dem auslösenden Ereignis Einspruch erhoben. Ungeachtet des Vorstehenden kann es Situationen geben, die eine sofortige Änderung der Bedingungen dieses DSA erfordern, die nur aus den in 7(b) dargelegten Gründen erfolgen darf und nur in gutem Glauben und nach Sicherstellung, dass die neuen oder geänderten Bedingungen nur auf diejenigen beschränkt sind, die erforderlich sind, um mit neuen anwendbaren Datenschutzgesetzen, Rechtsprechung oder von relevanten Datenschutzbehörden herausgegebenen Richtlinien in Einklang zu kommen.
	2. Für den Fall, dass eines der folgenden Szenarien eintritt, stimmen die Parteien sofort den neuesten Bedingungen zu, die unter der oben genannten Adresse veröffentlicht sind, es sei denn, es wird innerhalb von 30 Tagen nach Bekanntgabe der neuen Bedingungen durch das Unternehmen an alle Einheiten, die angefordert haben, benachrichtigt zu werden, bei privacy\_updates@msd.com Einspruch erhoben:

		1. das anwendbare Datenschutzgesetz wurde auf eine Weise aktualisiert, bei der die bestehenden vertraglichen Bedingungen dieses DSA nicht ausreichen, um den Anforderungen des aktualisierten Gesetzes gerecht zu werden,
		2. es gibt eine Änderung im anwendbaren Datenschutzgesetz, und die Parteien haben ein vernünftiges und legitimes Interesse daran, diese Bedingungen aufgrund der Gesetzesänderung zu ändern, zum Beispiel und ohne Einschränkung, durch Entfernen von Anforderungen, die nicht mehr notwendig sind, oder
		3. es gibt eine neue Rechtsprechung oder Richtlinien von relevanten Datenschutzbehörden, die eine vergleichbare Wirkung wie eine Gesetzesänderung gemäß (i) oder (ii) oben haben.
8. *Anwendbarkeit von Anhängen*. Die hier als Anlage 2 beigefügten Standardvertragsklauseln und die als Anlage 3 beigefügten Ergänzungen gelten nur in dem Umfang, in dem sie nach geltendem Datenschutzrecht erforderlich sind. Die Parteien verpflichten sich, diese Klauseln und Zusätze nur insoweit einzuhalten, als sie mit den Anforderungen des anwendbaren Datenschutzrechts in der jeweiligen Rechtsordnung übereinstimmen und durch diese erforderlich sind.
9. *Mitteilungen*. Mitteilungen im Rahmen dieser DSA (jeweils als „Mitteilung“ bezeichnet) müssen in schriftlicher Form erfolgen. Mitteilungen im Rahmen dieser DSA müssen in Übereinstimmung mit den Bestimmungen der jeweiligen Vereinbarung erfolgen, zusammen mit einer Kopie an das Unternehmen per E-Mail an msd\_privacy\_office@msd.com, mit dem Betreff „Mitteilung des Anbieters zur DSA“ oder im Falle einer Verletzung des Schutzes personenbezogener Daten „Dringend: Mitteilung der Verletzung des Schutzes personenbezogener Daten“.

**ANHANG 1 – Sicherheitsmaßnahmen in der Informationstechnologie**

1. Definitionen – Bei Verwendung in dieser Anlage hat jeder der folgenden definierten Begriffe die unten für diesen Begriff gegebene Definition. Definierte Begriffe, die in dieser Anlage verwendet, aber hierin nicht definiert werden, haben die im Vertrag an anderer Stelle festgelegte Bedeutung.
	1. „Unternehmensinformationen“ bezeichnet alle Informationen des Unternehmens oder eines seiner verbundenen Unternehmen oder deren jeweiligen Lieferanten, Kunden oder anderen Geschäftspartner, die vom Lieferanten oder einem seiner Drittanbieter-Dienstleister im Zusammenhang mit den Dienstleistungen bereitgestellt, erhalten, erstellt oder generiert oder anderweitig verarbeitet werden und alle anderen Informationen, die gemäß dem Vertrag als vertraulich zu behandeln sind.
	2. „Datenverstoß“ bezeichnet eine versehentliche oder unbefugte Zerstörung, Verlust, Veränderung, Nutzung, Übertragung oder Offenlegung von oder Zugang zu Unternehmensinformationen.
	3. „Endpunkt“ bezeichnet jeden Computer, einschließlich Laptop oder Desktop, mobiles Gerät, Laborequipment, Server oder anderes Gerät auf den Lieferantensystemen, einschließlich solcher, die auf einer externen Drittanbieterseite gehostet werden (z.B. Cloud-Anbieter).
	4. „Benachrichtigungsereignis“ bezeichnet jedes Ereignis, einschließlich eines Datenverstoßes, das die Benachrichtigung von Personen oder Einheiten nach geltendem Recht erfordert.
	5. „Sicherheitsereignis“ bezeichnet jeden A) Datenverstoß, (B) Benachrichtigungsereignis, (C) unbefugten Zugriff auf oder Störung der Betriebsabläufe der Lieferantensysteme oder (D) Verstoß gegen die Sicherheitsverpflichtungen des Lieferanten gemäß dieser Anlage, dem Vertrag oder geltendem Recht.
	6. „Betreffende Software“ bezeichnet jede Software, die im Zusammenhang mit den Dienstleistungen bereitgestellt oder verwendet wird, einschließlich jeder Software, die auf einem Computer, einschließlich Laptop oder Desktop, mobilem Gerät, Laborequipment, Server, anderem Gerät oder anderer Komponente der Informationssysteme des Unternehmens oder eines seiner verbundenen Unternehmen geliefert oder installiert wird.
	7. „Lieferantensysteme“ bezeichnet die Netzwerke des Lieferanten und alle Systeme, einschließlich der betreffenden Software, (A) die im Zusammenhang mit den Dienstleistungen bereitgestellt oder verwendet werden, (B) auf denen Unternehmensinformationen oder Lieferungen oder laufende Arbeiten für das Unternehmen oder seine verbundenen Unternehmen gespeichert oder anderweitig verarbeitet werden oder von denen aus sie zugänglich sind, (C) die mit den Informationen, Netzwerken oder anderen Systemen des Unternehmens oder seiner verbundenen Unternehmen verbunden sind oder von denen aus diese zugänglich sind, oder (D) mit denen die vorstehenden Punkte verbunden sind oder von denen aus sie zugänglich sind.
2. Netzwerksicherheit - Der Lieferant muss Netzwerksicherheitsrichtlinien, -verfahren und -kontrollen aufrechterhalten und Netzwerksicherheitsaktivitäten durchführen, die den Best Practices in der Branche des Lieferanten entsprechen, mindestens jedoch die Bereitstellung von Netzwerk-Firewalls, Kontrollen zur Erkennung und Verhinderung von Eindringlingen, Kontrollen zum Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) und regelmäßig durchgeführte Schwachstellenbewertungen und Penetrationstests umfassen, in Übereinstimmung mit den Best Practices in der Branche des Lieferanten (aber nicht weniger häufig als jährlich). In keinem Fall dürfen die Netzwerksicherheitsrichtlinien, -verfahren oder -kontrollen des Lieferanten, die zum Schutz von Unternehmensinformationen und Lieferantensystemen angewendet werden, weniger streng und schützend sein als die vom Lieferanten zum Schutz seiner eigenen Informationen und seiner anderen Systeme ähnlicher Art angewendeten.
3. Anwendungssicherheit - Je nach Art der erbrachten Dienstleistungen muss der Lieferant, falls zutreffend, Softwareentwicklungslebenszyklusprozesse und -kontrollen ("SDLC-Prozess") haben, die die Entwicklung von und Änderungen an jeglicher Lieferantensoftware regeln, einschließlich Updates, Upgrades, Patches, Verbesserungen, Fehlerbehebungen, Modifikationen, Verbesserungen, Korrekturen, Revisionen, Releases und andere Änderungen. Der SDLC-Prozess muss mindestens anerkannte und vergleichbare Industriestandards für sichere Softwareentwicklungspraktiken enthalten. Der Lieferant muss einen Patch-Management-Prozess befolgen, der sicherstellt, dass die Informationssysteme des Lieferanten mit angemessener Sicherheit und Funktionalität auf dem neuesten Stand sind. Der Lieferant muss zeitnah, entsprechend dem Risiko und innerhalb der in den Richtlinien und Verfahren des Lieferanten vorgesehenen Fristen, jede identifizierte Schwachstelle beheben und erneut testen.
4. Datensicherheit - Je nach Art der erbrachten Dienstleistungen muss der Lieferant, falls zutreffend, Unternehmensinformationen gemäß anerkannten und vergleichbaren Branchenpraktiken und -standards, wie sie beispielsweise in Absatz 11 (einschließlich PCI DSS, falls zutreffend) und in Übereinstimmung mit allen Gesetzen, behandeln, speichern und sonst verarbeiten. Der Lieferant muss angemessene Schutzmaßnahmen gegen einen Datenverstoß einrichten und aufrechterhalten. Zusätzlich zu und ohne Einschränkung anderer Verpflichtungen des Lieferanten muss der Lieferant alle Unternehmensinformationen gemäß den besten Praktiken in der Branche des Lieferanten und in Übereinstellung mit allen Gesetzen speichern und Sicherheitsmaßnahmen verwenden, die den besten Praktiken in der Branche des Lieferanten entsprechen, einschließlich Verschlüsselung und Firewalls, um Unternehmensinformationen vor einem Datenverstoß zu schützen. Wenn der Lieferant Unternehmensinformationen in einer externen Einrichtung speichert, muss der Lieferant alle Bedingungen in der Vereinbarung oder in einer im Zusammenhang mit der Vereinbarung abgeschlossenen Vereinbarung erfüllt haben, die sich auf die Offenlegung von Unternehmensinformationen gegenüber Dritten oder das Einbeziehen von Dritten zur Bereitstellung oder Unterstützung von Produkten oder Dienstleistungen beziehen, und der Lieferant muss eine externe Speichereinrichtung verwenden, die für das Unternehmen akzeptabel ist und die, ohne die vorstehenden Bestimmungen einzuschränken, vollständig alle Bestimmungen dieses Anhangs einhält. Darüber hinaus muss der Anbieter einer solchen externen Speichereinrichtung durch eine schriftliche Vertraulichkeitsvereinbarung zwischen dem Lieferanten und dem Anbieter gebunden sein, die Bedingungen enthält, die nicht weniger streng sind als die in der Vereinbarung oder einer im Zusammenhang mit der Vereinbarung abgeschlossenen Vereinbarung und die alle darin gespeicherten Unternehmensinformationen schützt.
5. Datenspeicherung - Je nach Art der erbrachten Dienstleistungen werden alle Unternehmensinformationen, falls zutreffend, ausschließlich auf den dafür vorgesehenen Rechen- und Speicherressourcen des Lieferanten behandelt, gespeichert und sonst verarbeitet. Unternehmensinformationen werden nur dann auf einem Laptop oder Mobilgerät behandelt, gespeichert oder sonst verarbeitet oder darauf übertragen, wenn (A) es sich um einen Laptop oder ein Mobilgerät des Lieferanten handelt, (B) der Lieferant alle Unternehmensinformationen auf diesem Laptop oder Mobilgerät gemäß den Verschlüsselungsstandards in Absatz 7 unten verschlüsselt und (C) dieser Laptop oder dieses Mobilgerät Endpunkt-Kontrollen unterliegt, die mit anerkannten und vergleichbaren Branchenpraktiken und -standards übereinstimmen, wie sie beispielsweise in Absatz 11 festgelegt sind. Unternehmensinformationen werden nicht auf einem tragbaren Gerät behandelt, gespeichert oder sonst verarbeitet, außer wie im vorhergehenden Satz vorgesehen. Der Lieferant muss alle Backups von Unternehmensinformationen als Teil seiner dafür vorgesehenen Backup- und Wiederherstellungsprozesse speichern, und solche Backups von Unternehmensinformationen müssen gemäß diesem Anhang verschlüsselt werden, einschließlich der Anforderungen dieses Absatzes 5 und Absatz 7 unten.
6. Datenübertragung - Je nach Art der erbrachten Dienstleistungen, falls zutreffend, erfolgt jede elektronische Übertragung oder der Austausch von Unternehmensinformationen über sichere Mittel (unter Verwendung von HTTPS oder SFTP oder Äquivalent), die mit anerkannten und vergleichbaren Branchenpraktiken und -standards übereinstimmen, wie sie in Absatz 11 festgelegt sind, und ausschließlich gemäß Absatz 7 unten.
7. Datenverschlüsselung - Je nach Art der erbrachten Dienstleistungen, falls zutreffend, zusätzlich zu und ohne Einschränkung anderer Verpflichtungen des Lieferanten, stimmt der Lieferant zu, dass alle Unternehmensinformationen, die aus personenbezogenen Daten bestehen, die gemäß einem Gesetz geschützt sind, oder aus Informationen, die gemäß dem aktuellen Payment Card Industry Data Protection Standard geschützt sind, einschließlich aller Sicherungsdaten des Unternehmens, in verschlüsselter Form aufbewahrt werden, unter Verwendung einer kommerziell unterstützten Verschlüsselungslösung. Der Lieferant stimmt zu, dass Verschlüsselungslösungen eingesetzt werden, die Unternehmensinformationen in Übereinstimmung mit anerkannten und vergleichbaren Branchenpraktiken und -standards verschlüsseln, wie sie in Absatz 11 festgelegt sind, jedoch mit mindestens einem 128-Bit-Schlüssel für symmetrische Verschlüsselung und einer 2048 (oder größer) Bit Schlüssellänge für asymmetrische Verschlüsselung.
8. Daten-Wiederverwendung - Je nach Art der erbrachten Dienstleistungen, falls zutreffend, wird der Lieferant alle Unternehmensinformationen ausschließlich zum Zwecke der Erbringung der Dienstleistungen verwenden. Der Lieferant darf keine Unternehmensinformationen verteilen, umwidmen oder über andere Anwendungen, Umgebungen oder Geschäftseinheiten des Lieferanten teilen.
9. Ende der Vereinbarung Datenhandhabung - Je nach Art der erbrachten Dienstleistungen, falls zutreffend, zusätzlich zu und ohne Einschränkung anderer Verpflichtungen des Lieferanten, wird auf Anfrage des Unternehmens und sofern im Vertrag nicht anders vorgesehen, bei Ablauf oder vorzeitiger Beendigung des Vertrags alle Unternehmensinformationen, die sich im Besitz oder unter der Kontrolle des Lieferanten oder eines seiner verbundenen Unternehmen, Subunternehmer, Dienstleister, Agenten oder sonstigen Berater befinden, zerstört oder zurückgegeben, je nach Wahl des Unternehmens.
10. Sicherheitsverletzungsbenachrichtigung - Zusätzlich zu und ohne Einschränkung anderer Verpflichtungen des Lieferanten, wird der Lieferant das Unternehmen innerhalb von 24 Stunden nach Kenntnisnahme eines tatsächlichen oder vernünftigerweise vermuteten Sicherheitsereignisses darüber informieren. Der Lieferant wird das Unternehmen über ein solches tatsächliches oder vernünftigerweise vermutetes Sicherheitsereignis informieren, indem er das Sicherheitsteam des Unternehmens telefonisch (+1-704-345-6700 – Option 1 wählen) und per E-Mail Global Operations Center globalopscnt@merck.com kontaktiert. Der Lieferant wird Informationen und Unterstützung bereitstellen, die das Unternehmen in Bezug auf ein Sicherheitsereignis vernünftigerweise anfordern kann, einschließlich Informationen über die Ursache.
11. Branchenstandards - Allgemein anerkannte Branchenstandards umfassen, sind aber nicht beschränkt auf die aktuellen Standards und Benchmarks, die von den folgenden Stellen festgelegt und gepflegt werden:
	1. Center for Internet Security - siehe [http://www.cisecurity.org](http://www.cisecurity.org/)
	2. Payment Card Industry / Data Security Standards (PCI/DSS) – siehe <http://www.pcisecuritystandards.org/>
	3. National Institute for Standards and Technology - siehe [http://csrc.nist.gov](http://csrc.nist.gov/)
	4. Federal Information Security Management Act (FISMA) - siehe [http://csrc.nist.gov](http://csrc.nist.gov/)
	5. ISO/IEC 27000-series - siehe <http://www.iso27001security.com/>
	6. Organization for the Advancement of Structured Information Standards (OASIS) – siehe <http://www.oasis-open.org/>
	7. The Open Web Application Security Project’s (OWASP) – siehe [http://www.owasp.org](http://www.owasp.org/)
	8. Die CWE (Common Weakness Enumeration) - siehe [http://cwe.mitre.org](http://cwe.mitre.org/) oder CWE/SANS Top 25 Programmierfehler - <http://cwe.mitre.org/top25/>
	9. Das SANS-Institut - siehe [http://www.sans.org](http://www.sans.org/)
	10. Die gefährlichsten Softwarefehler <http://www.sans.org/top25-programming-errors/>

Auf angemessene Anfrage des Unternehmens hin, soll der Lieferant dem Unternehmen die Überprüfung der Einhaltung der oben genannten Anforderungen durch den Lieferanten ermöglichen. Der Lieferant soll etwaige Nichteinhaltungen der Anforderungen so schnell wie möglich beheben.

**ANHANG 2**

Für den Fall, dass das Unternehmen personenbezogene Daten in einer Weise exportiert, die Modul 1 der Standardvertragsklauseln erfordert, gelten die folgenden Bedingungen:

*Der Haupttext von Modul 1 (Verantwortlicher an Verantwortlicher) der Standardvertragsklauseln, die dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 beigefügt sind, wird hiermit durch Verweis aufgenommen. Optionale Aspekte werden im Folgenden beschrieben:*

1. *Klausel 7 (Andockklausel) entfällt.*
2. *Für Klausel 11 entfällt der optionale Text.*
3. *Für Klausel 17 wird Option 1 gewählt, wobei der Mitgliedstaat die Niederlande ist.*
4. *Für Klausel 18 ist der Gerichtsstand die Niederlande.*

**ANHANG I ZU ANLAGE 2**

**A. LISTE DER PARTEIEN**

*Siehe Vereinbarung*

**B. BESCHREIBUNG DER ÜBERTRAGUNG**

*Siehe Anlage zur Vereinbarung mit dem Titel „Die Datenverarbeitung im Einzelnen“.*

**C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE**

****Commission Nationale de l'Informatique et des Libertés - CNIL****
3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Website: [**http://www.cnil.fr/**](http://www.cnil.fr/)

**ANHANG 2 ZU ANLAGE 2 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN**

Siehe Anhang 1 der DSA, dem diese Klauseln beigefügt sind. Darüber hinaus stellt der Datenimporteur sicher, dass alle personenbezogenen Daten pseudonymisiert und gegebenenfalls verschlüsselt werden. Außerdem garantieren der Datenimporteur und seine verbundenen Unternehmen, wenn sie eine Anfrage von einer Regierungsbehörde in Bezug auf die personenbezogenen Daten erhalten, die Gegenstand dieser Klauseln sind, dass (i) Zugriffsforderungen von Nachrichtendiensten oder ähnlichen Behörden in den USA oder anderswo auf die in Anhang 1B beschriebenen personenbezogenen Daten und (ii) jede „Offenlegungsplicht“ betreffend diese Daten vom Datenimporteur und seinen verbundenen Unternehmen in Übereinstimmung mit den geltenden Gesetzen und Vorschriften vor der Extraktion angefochten werden.

**ANHANG 3**

**Zusätzliche gesetzliche Anforderungen auf Staats-, Landes-, Regional- und Provinzebene**

**ERGÄNZUNG FÜR DAS VEREINIGTE KÖNIGREICH: Data Protection Act 2018**

Dieser Anhang 3 enthält hiermit durch Verweis das Addendum für den internationalen Datentransfer zu den Standardvertragsklauseln der EU-Kommission, Version B1.0, in der Fassung vom 21. März 2022, und gilt als von allen Vertragsparteien vollständig ausgeführt, so dass alle anwendbaren Übermittlungen gemäß der DSA abgedeckt sind, einschließlich aller obligatorischen Klauseln von Teil 2.

**ERGÄNZUNG FÜR DIE SCHWEIZ: FADP**

1. Soweit die in Anhang 2 beschriebenen Datenübermittlungen dem DSG unterliegen, sind Verweise auf die DSGVO als Verweise auf das Schweizer Bundesdatenschutzgesetz („DSG“) zu verstehen.
2. Solange das DSG dies vorschreibt, werden die personenbezogenen Daten juristischer Personen im Sinne dieser Klauseln in gleicher Weise geschützt wie natürliche Personen, die betroffene Personen sind.
3. Klausel 13: Parallele Aufsicht
	1. Sofern die Datenübermittlung durch das DSG geregelt ist: ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte („EDÖB“) die zuständige Aufsichtsbehörde;
	2. Sofern die Datenübermittlung durch die DSGVO geregelt ist: gelten die Kriterien von Klausel 13(a).
4. Klausel 18(c): Wahl des Gerichtsstands und der Gerichtsbarkeit: Eine betroffene Person, die ihren gewöhnlichen Aufenthalt in der Schweiz hat, kann auch vor den Gerichten der Schweiz gegen den Datenexporteur und/oder Datenimporteur Klage erheben.

**ERGÄNZUNG FÜR KANADA: Quebec Law 25**

* + - 1. Jede Mitteilung, die gemäß dieser DSA in Bezug auf eine Verletzung des Schutzes personenbezogener Daten erforderlich ist, und jede ähnliche Mitteilung, die gemäß der Vereinbarung erforderlich ist, ist auch für jedes Ereignis erforderlich, das eine Verletzung oder versuchte Verletzung dieser DSA durch den Anbieter darstellt.
			2. Falls im Zusammenhang mit den Bedingungen dieser DSA die Einholung von Einwilligungen erforderlich ist, muss der Anbieter auch die Nachweise für alle Einwilligungen für drei (3) Jahre nach Beendigung der Vereinbarung aufbewahren.

**ZUSATZVEREINBARUNG DER VEREINIGTEN ARABISCHEN EMIRATE: Bundesgesetz Nr. 45 von 2021 über den Schutz personenbezogener Daten**

1. Soweit die in Anhang 2 beschriebenen Datenübertragungen dem Bundesgesetz Nr. 45 von 2021 der Vereinigten Arabischen Emirate über den Schutz personenbezogener Daten („PDPL“) unterliegen, gilt Folgendes: Solange und bis das Datenamt der VAE eigene Standardvertragsklauseln erlässt, um die Übermittlung personenbezogener Daten außerhalb der Vereinigten Arabischen Emirate zu legitimieren, und die Parteien solche Standardvertragsklauseln abgeschlossen haben, vereinbaren die Parteien, dass die dem Anhang 2 beigefügten Standardvertragsklauseln mutatis mutandis in Bezug auf solche Übertragungen gelten, um angemessene Sicherheitsvorkehrungen für die personenbezogenen Daten und die betroffenen Personen zu gewährleisten. Zu diesem Zweck: a. Verweise auf die „Verordnung (EU) 2016/679“, die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzverordnung)“ und „diese Verordnung“ werden durch „PDPL“ ersetzt. b. Verweise auf spezifische Artikel der „Verordnung (EU) 2016/679“ werden durch die entsprechenden Artikel oder Abschnitte der PDPL ersetzt. c. Verweise auf die „Europäische Union“, „Union“, „EU“, „EU-Mitgliedstaat“, „Mitgliedstaat“ und „EU oder Mitgliedstaat“ werden alle durch die „Vereinigten Arabischen Emirate“ ersetzt. d. Die „zuständige Aufsichtsbehörde“ und die „Aufsichtsbehörde“ werden beide durch das „Datenamt“ ersetzt. e. Jede Streitigkeit aus den Standardvertragsklauseln unterliegt den Gesetzen der Vereinigten Arabischen Emirate und wird von den Gerichten der Vereinigten Arabischen Emirate entschieden. Die Parteien vereinbaren, sich der Zuständigkeit dieser Gerichte zu unterwerfen. f. Im Falle eines Widerspruchs oder Konflikts zwischen der PDPL und den dem Anhang 2 beigefügten Standardvertragsklauseln gilt die PDPL. g. Wenn der Inhalt der dem Anhang 2 beigefügten Standardvertragsklauseln unklar ist, soweit er auf Übertragungen personenbezogener Daten außerhalb der VAE anwendbar ist, oder es mehrere Bedeutungen gibt, gilt die Bedeutung, die am ehesten mit der PDPL übereinstimmt.
2. Wenn das Datenamt der VAE eigene Standardvertragsklauseln erlässt, um die Übermittlung personenbezogener Daten außerhalb der Vereinigten Arabischen Emirate zu legitimieren, werden die Parteien nach Treu und Glauben verhandeln, um die Standardvertragsklauseln so bald wie möglich zu vereinbaren und umzusetzen. Wenn die Parteien Standardvertragsklauseln gemäß dem vorstehenden Satz abschließen, ersetzen diese Standardvertragsklauseln in Bezug auf Übertragungen personenbezogener Daten, die der PDPL unterliegen, außerhalb der Vereinigten Arabischen Emirate die dem Anhang 2 beigefügten Standardvertragsklauseln als die angemessenen Sicherheitsvorkehrungen, die zur Bereitstellung angemessener Sicherheitsvorkehrungen für die personenbezogenen Daten und die betroffenen Personen in Bezug auf die Übertragungen umgesetzt werden.
3. Das Unternehmen kann seine Zustimmung zur Bindung an die dem Anhang 2 beigefügten Standardvertragsklauseln durch schriftliche Mitteilung an den Lieferanten widerrufen, wenn das Datenamt eine Angemessenheitsentscheidung trifft, die die Übermittlung personenbezogener Daten abdeckt, auf die die Standardvertragsklauseln Anwendung finden, oder wenn das Unternehmen anderweitig feststellt, dass andere angemessene Sicherheitsvorkehrungen in Bezug auf die Übermittlung gelten. Ab dem Datum einer solchen Mitteilung des Unternehmens gemäß dem vorstehenden Satz gelten die dem Anhang 2 beigefügten Standardvertragsklauseln nicht mehr für Übertragungen personenbezogener Daten, die der PDPL unterliegen, außerhalb der Vereinigten Arabischen Emirate.

**BRASILIEN-ANHANG: LGPD - Standardvertragsklauseln**

Die brasilianischen Standardvertragsklauseln ("SCCs") gemäß dem Allgemeinen Datenschutzgesetz (Lei Geral de Proteção de Dados – “LGPD”) sind einzuhalten, wenn Daten von brasilianischen Einwohnern verarbeitet werden, oder wenn eine Datenübertragung deren Anwendung erforderlich macht. Die Parteien stimmen zu, die SCCs in ihrer Gesamtheit zu übernehmen, wie sie von der brasilianischen Datenschutzbehörde (“ANPD”) herausgegeben wurden, es sei denn, sie werden gemäß den in den Klauseln ausdrücklich erlaubten Bedingungen geändert. Solche SCCs sind durch Bezugnahme in das Abkommen aufgenommen, wobei die folgenden Optionen ausgewählt wurden, wenn mehr als eine Textoption vorliegt:

OPTION B wird für Abschnitt 3.1 gewählt. Der Importeur kann eine Weiterübertragung personenbezogener Daten im Rahmen der internationalen Datenübertragung gemäß diesen Klauseln vornehmen, unter den nachstehend beschriebenen Bedingungen und den Bestimmungen der KLAUSEL 18.

OPTION A wird für Abschnitt 4.1 gewählt. Unbeschadet der Pflicht zur gegenseitigen Unterstützung und der allgemeinen Verpflichtungen der Parteien ist die unten bezeichnete Partei hauptsächlich dafür verantwortlich, die in diesen Klauseln festgelegten Verpflichtungen einzuhalten:

a) Verantwortlich für die Veröffentlichung des in KLAUSEL 14 vorgesehenen Dokuments:

[x] Exporteur [ ] Importeur

b) Verantwortlich für die Bearbeitung von Anfragen der betroffenen Personen gemäß KLAUSEL 15:

[x] Exporteur [ ] Importeur

c) Verantwortlich für die Meldung des in KLAUSEL 16 vorgesehenen Sicherheitsvorfalls:

[x] Exporteur [ ] Importeur

**SAUDI-ARABIEN-ANHANG: PDPL - Standardvertragsklauseln**

Die saudi-arabischen Standardvertragsklauseln („SCCs“) gemäß dem Datenschutzgesetz („PDPL“) sind zu integrieren, wenn Daten von saudischen Einwohnern verarbeitet werden, wenn eine Datenübertragung der saudi-arabischen Gerichtsbarkeit unterliegt oder wenn das saudi-arabische Recht die Einhaltung der saudi-arabischen SCCs erfordert. Die Version der SCCs, die mit dem im Anhang 2 beschriebenen Vorlage-Typ übereinstimmt, ist vollständig anwendbar und wird durch Verweis in das Abkommen aufgenommen.