**Auftragsverarbeitungsvertrag**

Dieser Auftragsverarbeitungsvertrag **(„AVV“)** spiegelt die Vereinbarung der Parteien in Bezug auf die Bedingungen wider, die die Verarbeitung Personenbezogener Daten im Auftrag des Kunden im Rahmen jeder gültigen schriftlichen Vereinbarung zwischen dem Kunden und Dynatrace festlegen, die die Nutzung der Dynatrace-Angebote (entgeltlich oder anderweitig) regelt, sowie aller zugehörigen Bestellformulare, Anhänge und Leistungsbeschreibungen (zusammen die **„Vereinbarung“**). Dieser AVV tritt an dem Datum in Kraft, an dem er von beiden Parteien unterzeichnet wurde (das **„Datum des Inkrafttretens“**).

Dieser AVV unterliegt den Bedingungen der Vereinbarung und wird vollumfänglich Bestandteil dieser Vereinbarung. Dieser AVV ersetzt alle bestehenden Auftragsverarbeitungsverträge, sofern hierin nicht ausdrücklich etwas anderes angegeben ist. Im Falle eines Widerspruchs zwischen diesem AVV und einer anderen Bestimmung der Vereinbarung in Bezug auf Personenbezogene Daten gilt dieser AVV. Großgeschriebene Begriffe, die in diesem AVV verwendet, aber nicht definiert werden, haben die gleiche Bedeutung wie im Subscription Agreement (Abonnementvertrag), der unter https://assets.dynatrace.com/global/legal/Online-SA-April-2023-German.pdf zu finden ist.

**1. Definitionen.**

(a) „**APPI**“ bezeichnet Japans Datenschutzgesetz (Act on the Protection of Personal Information) (Gesetz Nr. 57 von 2003 in der geänderten Fassung von 2016).

(b) „**Datenschutzgesetz**“ bezeichnet alle Datenschutzgesetze und -vorschriften, die für die Verarbeitung Personenbezogener Kundendaten durch Dynatrace im Rahmen der Vereinbarung gelten.

(c) „**Verantwortlicher**“ hat die gleiche Bedeutung wie in den geltenden Datenschutzgesetzen und schließt „Datenbankbesitzer“ gemäß dem israelischen Datenschutzgesetz und „Unternehmen“ gemäß dem jeweiligen anwendbaren Datenschutzgesetz der US-Bundesstaaten ein.

(d) „**Personenbezogene Kundendaten**“ bezeichnet alle Personenbezogenen Daten, die vom oder im Auftrag des Kunden im Rahmen der Nutzung der Dynatrace-Angebote übermittelt, gespeichert, gepostet, angezeigt oder anderweitig übermittelt werden; und schließt Personenbezogene Daten (wie Eingeschränkte Informationen) aus, die vom oder im Auftrag des Kunden unter Verstoß gegen eine Bestimmung der Vereinbarung und/oder dieses AVV übermittelt, gespeichert, gepostet, angezeigt oder anderweitig übermittelt werden.

(e) „**Dynatrace Group**“ bezeichnet eine oder mehrere Einheiten von Dynatrace LLC, einer Gesellschaft mit beschränkter Haftung in Delaware, und ihren verbundenen Unternehmen, die Dynatrace bei der Bereitstellung der Dynatrace-Angebote und/oder damit verbundenen Support- oder Dienstleistungen im Rahmen der Vereinbarung und dieses AVV unterstützen können.

(f) „**Europa**“ bezeichnet die Europäische Union, den Europäischen Wirtschaftsraum („EWR“) und/oder ihre Mitgliedsstaaten, die Schweiz und das Vereinigte Königreich.

(g) „**DSGVO**“ bezeichnet die Verordnung 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung).

(h) „**LGPD**“ bezeichnet das Lei Geral de Proteção de Dados Pessoais (Datenschutzgesetz in Brasilien).

(i) „**Verletzung des Schutzes Personenbezogener Daten**“ bezeichnet eine Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Vernichtung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unberechtigten Zugriff auf Personenbezogene Kundendaten führt, während diese von Dynatrace übermittelt, gespeichert oder anderweitig verarbeitet werden.

(j) „**PIPL**“ bezeichnet das chinesische Gesetz zum Schutz Personenbezogener Daten (Personal Information Protection Law).

(k) „**Personenbezogene Daten**“ bezeichnet „personenbezogene Daten“ oder „personenbezogene Informationen“ im Sinne der Definition in den geltenden Datenschutzgesetzen, die Dynatrace im Auftrag des Kunden erhebt oder erhält. Zu den Personenbezogenen Daten gehören keine Informationen, die Dynatrace unabhängig von der Erfüllung seiner jeweiligen Verpflichtungen aus der Vereinbarung mit dem Kunden erhält oder verarbeitet.

(l) „**Auftragsverarbeiter**“ hat die gleiche Bedeutung wie in geltenden Datenschutzgesetzen und umfasst den „Inhaber“ gemäß der Definition im israelischen Datenschutzgesetz und den „Dienstleister“ gemäß dem jeweils anwendbaren Datenschutzgesetz der US-Bundesstaaten.

(m) „**Standardvertragsklauseln**“ bezeichnet die durch den Beschluss 2021/914/EU der EU-Kommission veröffentlichten Standardvertragsklauseln, die hier durch Verweis in ihrer jeweils aktualisierten, geänderten oder ersetzten Fassung aufgenommen werden.

(n) „**Unterauftragsverarbeiter**“ bezeichnet Auftragsverarbeiter, die von Dynatrace oder Mitgliedern der Dynatrace Group beauftragt werden, um Dynatrace zu ermöglichen, die Dynatrace-Angebote gemäß den Bedingungen der Vereinbarung oder dieses AVV zu liefern/zu erbringen.

(o) „**Aufsichtsbehörde**“ ist die Regierungsbehörde, das Ministerium oder eine andere zuständige Organisation, die für die Verarbeitung Personenbezogener Daten im Rahmen dieses AVV zuständig ist.

(p) „**UK-Nachtrag**“ bezeichnet den Nachtrag zur internationalen Datenübertragung zu den Standardvertragsklauseln der EU-Kommission, die vom Büro des britischen Informationsbeauftragten gemäß S119A (1) Data Protection Act 2018, in der jeweils aktualisierten, geänderten oder ersetzten Fassung.

(q) **„Unternehmen“,** „**Verantwortlicher**“, „**Verbraucher“,** „**Auftragsverarbeiter**“, „**Dienstleister**“, „**betroffene Person**“, **„Verkauf“,** und „**Verarbeitung**“ (und „**verarbeiten**“) haben die Bedeutung, die ihnen nach dem jeweils anwendbaren Datenschutzrecht zukommt.

## 2. Anwendbarkeit des AVV und der Rollen der Parteien

(a) Dieser AVV gilt für die Verarbeitung Personenbezogener Kundendaten durch Dynatrace im Auftrag des Kunden, um die in der Vereinbarung und diesem AVV enthaltenen Verpflichtungen zu erfüllen und Rechte auszuüben. Zur Klarstellung sei angemerkt, dass dieser AVV nicht für die Verarbeitung Personenbezogener Kundendaten durch Dynatrace als Verantwortlicher gilt.

(b) Der Kunde ist ein Verantwortlicher oder ein Auftragsverarbeiter und Dynatrace ist ein Auftragsverarbeiter. Soweit nach dem Datenschutzgesetz anwendbar, ernennt der Kunde Dynatrace als Auftragsverarbeiter, um die Personenbezogenen Kundendaten im Namen des Kunden zu verarbeiten.

## 3. Verarbeitung Personenbezogener Kundendaten

(a) Die Art und der Umfang der Verarbeitung Personenbezogener Kundendaten durch Dynatrace zur Bereitstellung der Dynatrace-Angebote wird vom Kunden bestimmt und kontrolliert und durch Anhang A ergänzt. Die Art, der Zweck und die Dauer der Verarbeitung sowie die Arten der erfassten Personenbezogenen Daten und Kategorien von betroffenen Personen, deren Personenbezogene Daten von Dynatrace verarbeitet werden können, sind in **Anhang A** zu diesem AVV beschrieben. Der Kunde bestätigt, dass Dynatrace keine Kenntnis von den tatsächlichen Daten oder Arten Personenbezogener Daten hat, die in den Kundendaten enthalten sind. Die Parteien vereinbaren, dass die vollständigen und endgültigen Anweisungen des Kunden über die Art und die Zwecke der Verarbeitung in Verbindung mit den Dynatrace-Angeboten in der Vereinbarung und in diesem AVV dargelegt sind.

(b) Alle Änderungen oder Modifikationen der Anweisungen müssen schriftlich mitgeteilt und von beiden Parteien bestätigt werden. Dynatrace wird den Kunden informieren, wenn die Verarbeitungsanweisungen des Kunden nach vernünftiger Einschätzung von Dynatrace wahrscheinlich gegen geltende Datenschutzgesetze verstoßen. In diesem Fall ist Dynatrace berechtigt, die Verarbeitung Personenbezogener Kundendaten, die nach Ansicht von Dynatrace gegen geltende Datenschutzgesetze verstoßen, zu verweigern, bis der Kunde seine Anweisungen so ändert, dass sie nicht mehr gegen diese Gesetze verstoßen.

(c) Soweit die Konfiguration der Dynatrace-Angebote durch den Kunden dazu führt, dass Dynatrace Personenbezogene Kundendaten erfasst, sichert der Kunde zu und gewährleistet, dass er jederzeit alle geltenden Datenschutzgesetze einhalten wird. Zwischen dem Kunden und Dynatrace ist der Kunde für Folgendes verantwortlich: (i) den Schutz Personenbezogener Kundendaten während der Nutzung von Dynatrace durch Konfiguration der Datenschutzeinstellungen von Dynatrace, wie unter ttps://docs.dynatrace.com/docs/manage/data-privacy-and-security beschrieben (Anweisungen von Dynatrace zur Konfiguration von Datenschutzeinstellungen), um den Umfang der von den Dynatrace-Angeboten zu erfassenden Personenbezogenen Kundendaten granular zu kontrollieren; (ii) die Genauigkeit, Qualität und Rechtmäßigkeit personenbezogener Kundendaten, und die Mittel, mit denen der Kunde oder ein relevanter Dritter Personenbezogene Daten erhalten hat.

(d) Wenn der Kunde ein Auftragsverarbeiter ist, der im Auftrag eines dritten Verantwortlichen handelt, gewährleistet der Kunde Dynatrace, dass die Anweisungen und Handlungen des Kunden in Bezug auf diese Personenbezogenen Kundendaten, einschließlich der Ernennung von Dynatrace als weiteren Auftragsverarbeiter, vom jeweiligen Verantwortlichen genehmigt wurden.

(e) Der Kunde sichert zu und gewährleistet, dass: (i) er betroffenen Personen wie gesetzlich vorgeschrieben über seine Nutzung von Auftragsverarbeitern zur Verarbeitung ihrer Personenbezogenen Kundendaten, einschließlich Dynatrace, informiert, wobei er die betroffenen Personen gegebenenfalls auch über die Nutzung der Dynatrace-Angebote informiert; (ii) er während der Laufzeit alle notwendigen Rechte, Rechtsgrundlagen, Genehmigungen und/oder gültige Einwilligungen, einschließlich von den Betroffenen, für die Verarbeitung der Personenbezogenen Kundendaten durch Dynatrace gemäß der Vereinbarung erhalten hat und weiterhin erhält; (iii) die Nutzung der Dynatrace-Angebote durch den Kunden nicht gegen geltende Datenschutzgesetze oder andere anwendbare Gesetze oder Regelungen verstößt und einen solchen Verstoss nicht für Dynatrace verursacht, oder eine Verletzung von Vereinbarungen oder Verpflichtungen zwischen dem Kunden und Dritten verursacht.

(f) Der Kunde stellt Dynatrace nur die Personenbezogenen Kundendaten zur Verfügung, die für Dynatrace zur Erfüllung seiner Verpflichtungen aus der Vereinbarung in Bezug auf die Dynatrace-Angebote und alle damit verbundenen Dienstleistungen erforderlich sind. Der Kunde erkennt an, dass die Nutzung der Dynatrace-Angebote die Verarbeitung von Eingeschränkten Informationen nicht erfordert und nicht dafür geeignet ist und wird durch seine Nutzung der Dynatrace-Angebote keine Eingeschränkten Informationen zur Verarbeitung durch Dynatrace bereitstellen.

**4. Anfragen von Dritten.**

(a) Dynatrace-Angebote bieten dem Kunden die Funktionalität, auf Personenbezogene Kundendaten zuzugreifen, um Kunden bei Anfragen von betroffenen Personen, die ihre Rechte nach dem Datenschutzgesetz ausüben („Anfragen von betroffenen Personen“), oder bei Anfragen von Aufsichts- oder Justizbehörden in Bezug auf die Verarbeitung Personenbezogener Kundendaten zu unterstützen. Soweit der Kunde nicht in der Lage ist, auf die relevanten Personenbezogenen Kundendaten innerhalb der Dynatrace-Angebote zuzugreifen oder der Zugriff auf die Personenbezogenen Kundendaten keine ausreichende Unterstützung bietet, um solche Anfragen in Übereinstimmung mit dem Datenschutzrecht zu beantworten, und soweit dies durch das anwendbare Datenschutzrecht vorgeschrieben ist, erklärt sich Dynatrace auf Anfrage des Kunden bereit, dem Kunden angemessene Unterstützung zu leisten, um ihn in die Lage zu versetzen, auf Anfragen von betroffenen Personen oder von Aufsichts- oder Justizbehörden in Bezug auf die Verarbeitung Personenbezogener Kundendaten im Rahmen der Vereinbarung zu reagieren.

Wenn eine Anfrage in Bezug auf Personenbezogene Kundendaten direkt an Dynatrace gestellt wird, für die Dynatrace den Kunden als Verantwortlichen identifizieren kann, wird Dynatrace diese Mitteilung unverzüglich an den Kunden weiterleiten und ohne die ausdrückliche Genehmigung des Kunden nicht auf diese Anfrage antworten. Das Vorstehende verbietet Dynatrace nicht, mit einer betroffenen Person oder einer Aufsichts- oder Justizbehörde zu kommunizieren, wenn sich aus der Mitteilung nicht vernünftigerweise ergibt, dass sich die Anfrage auf den Kunden bezieht, oder wenn Dynatrace eine gesetzliche Verpflichtung hat, selbst zu antworten.

(b) Wenn Dynatrace aufgrund einer Anfrage einer Strafverfolgungsbehörde oder eines anderen Dritten gezwungen ist, Personenbezogene Daten offenzulegen, für die der Kunde der Verantwortliche ist, wird Dynatrace den Kunden über eine solche Anfrage informieren, bevor Dynatrace Zugang zu Personenbezogenen Daten gewährt und/oder diese zur Verfügung stellt, um dem Kunden zu ermöglichen, eine Schutzanordnung oder ein anderes angemessenes Rechtsmittel zu erwirken. Wenn es Dynatrace gesetzlich untersagt ist, den Kunden zu benachrichtigen, wird Dynatrace Maßnahmen ergreifen, um die Personenbezogenen Daten vor unzulässiger Offenlegung zu schützen, so als ob es sich um Vertrauliche Informationen von Dynatrace handeln würde, die angefordert werden.

5. **Unterstützung und Zusammenarbeit.** Vorbehaltlich der Art der Verarbeitung und der Dynatrace zur Verfügung stehenden Personenbezogenen Daten und soweit durch das anwendbare Datenschutzrecht vorgeschrieben, wird Dynatrace auf schriftliche Anfrage des Kunden dem Kunden angemessene Unterstützung und Informationen zur Verfügung stellen, wenn nach Einschätzung des Kunden die Art der von Dynatrace durchgeführten Verarbeitung eine Datenschutz-Folgenabschätzung und/oder eine vorherige Konsultation der relevanten Datenschutzbehörden erfordert, und dem Kunden angemessene Unterstützung bei der Einhaltung seiner anderen Verpflichtungen unter dem anwendbaren Datenschutzrecht in Bezug auf Datensicherheit und Benachrichtigung über Datenschutzverletzungen leisten, soweit dies auf die Verarbeitung der Personenbezogenen Kundendaten anwendbar ist. Der Kunde erstattet Dynatrace alle nicht vernachlässigbaren Kosten, die Dynatrace bei der Erfüllung seiner Verpflichtungen aus diesem Abschnitt entstehen.

6. **Nachweisliche Compliance.** Dynatrace verpflichtet sich, auf angemessene Anfrage des Kunden die Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung dieses AVV nachzuweisen.

7. **Audits und Bewertungen.**

(a) Soweit die anwendbaren Datenschutzgesetze dem Kunden ein Audit- oder Bewertungsrecht einräumen und vorbehaltlich des Umfangs dieses Rechts, kann der Kunde auf schriftliche Anfrage des Kunden und bis zu einmal pro Jahr in Übereinstimmung mit den geltenden Datenschutzgesetzen ein Audit oder eine Bewertung der Richtlinien, Verfahren und Aufzeichnungen von Dynatrace durchführen, die für die Verarbeitung Personenbezogener Kundendaten relevant sind.

(b) Um ein Audit anzufragen, muss der Kunde Dynatrace mindestens vier (4) Wochen vor dem vorgeschlagenen Auditdatum einen detaillierten Auditplan vorlegen, der den vorgeschlagenen Umfang, die Dauer und das Startdatum des Audits beschreibt. Dynatrace wird den Auditplan überprüfen und dem Kunden alle Bedenken oder Fragen mitteilen. Vor Beginn eines Audits vereinbaren die Parteien einen detaillierten Auditplan, einschließlich Gebühren, Zeitpunkt, Umfang der Kontrollen, vorzulegende Nachweise und Dauer. Wenn der angeforderte Auditumfang innerhalb der letzten zwölf Monate in einem ähnlichen Prüfungsbericht behandelt wird und Dynatrace bestätigt, dass es keine wesentlichen Änderungen bei den geprüften Kontrollen gibt, stimmt der Kunde zu, diese Ergebnisse anstelle der Anforderung einer Prüfung der vom Bericht erfassten Kontrollen zu akzeptieren.

(c) Jedes Audit oder jede Bewertung muss: (i) während der normalen Geschäftszeiten von Dynatrace durchgeführt werden; (ii) den Vertraulichkeitsverpflichtungen der Parteien unterliegen. Wenn ein Dritter den Audit durchführen soll, darf der Dritte kein Wettbewerber von Dynatrace sein, und dieser Dritte unterliegt der vorherigen Zustimmung von Dynatrace und muss vor der Durchführung des Audits eine schriftliche Vertraulichkeitsvereinbarung mit den Parteien abschließen.

(d) Alle Audits erfolgen auf Kosten des Kunden. Jede Anfrage an Dynatrace auf Unterstützung bei einem Audit gilt als separate Dienstleistung, wenn eine solche Prüfungsunterstützung die Nutzung von Ressourcen erfordert, die sich von denen unterscheiden, die für die Bereitstellung der Dynatrace-Angebote erforderlich sind, oder diese ergänzen. Dynatrace wird die schriftliche Bestätigung des Kunden einholen, dass er alle anwendbaren Gebühren zahlen wird, bevor es eine solche Prüfungsunterstützung leistet.

8. **Vertraulichkeit.** Dynatrace stellt sicher, dass alle Personen, die von Dynatrace ermächtigt werden, die Personenbezogenen Kundendaten zu verarbeiten (einschließlich seiner Mitarbeiter, Vertreter und Unterauftragnehmer), einer vertraglichen, gesetzlichen oder sonstigen verbindlichen Verpflichtung zur Vertraulichkeit unterliegen.

9. **Sicherheit**

(a) **Sicherheitsmaßnahmen.** Unter Berücksichtigung des Stands der Technik, der Kosten der Implementierung und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen hat Dynatrace geeignete technische und organisatorische Maßnahmen ergriffen und wird diese aufrechterhalten, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko der Verarbeitung Personenbezogener Kundendaten angemessen ist **(„Sicherheitsmaßnahmen“).** Der Kunde bestätigt, dass die Umsetzung der in **Anhang B** genannten Sicherheitsmaßnahmen durch Dynatrace ausreichend ist, um seinen Verpflichtungen aus diesem AVV nachzukommen. Ungeachtet des Vorstehenden erkennt der Kunde an und stimmt zu, dass er für seine eigene sichere Nutzung der Dynatrace-Angebote verantwortlich ist.

(b) **Verletzung des Schutzes Personenbezogener Daten.** Dynatrace benachrichtigt den Kunden ohne schuldhaftes Zögern und spätestens dann, wenn Dynatrace nach geltendem Datenschutzrecht dazu verpflichtet ist, nachdem das Unternehmen von einer Verletzung des Schutzes Personenbezogener Daten Kenntnis erlangt hat. Dynatrace wird umgehend eine Untersuchung der Umstände im Zusammenhang mit der Verletzung des Schutzes Personenbezogener Daten einleiten und dem Kunden seine Ergebnisse zur Verfügung stellen. Dynatrace wird sich bemühen, alle nach geltendem Datenschutzrecht erforderlichen Schritte zu unternehmen, um die Auswirkungen einer solchen Verletzung des Schutzes Personenbezogener Daten zu mindern. Auf Verlangen des Kunden und unter Berücksichtigung der Art der Verarbeitung und der Dynatrace zur Verfügung stehenden Informationen wird Dynatrace wirtschaftlich angemessene Schritte unternehmen, um den Kunden bei der Erfüllung seiner Verpflichtungen zu unterstützen, die erforderlich sind, um es dem Kunden zu ermöglichen, relevante Verletzungen des Schutzes Personenbezogener Daten gegenüber zuständigen Behörden und/oder betroffenen Personen zu melden, wenn der Kunde gemäß geltendem Datenschutzrecht dazu verpflichtet ist. Die Benachrichtigung über eine Verletzung des Schutzes Personenbezogener Daten erfolgt an einen oder mehrere Administratoren des Kunden auf eine von Dynatrace gewählte Weise, einschließlich per E-Mail. Es liegt in der alleinigen Verantwortung des Kunden, sicherzustellen, dass die Administratoren des Kunden korrekte Kontaktinformationen im Online-Portal pflegen oder wie anderweitig von Dynatrace in einer schriftlichen Mitteilung an den/die Administrator(en) des Kunden gefordert. Dynatraces Verpflichtung, eine Verletzung des Schutzes Personenbezogener Daten im Rahmen dieses Abschnitts zu melden oder darauf zu reagieren, ist keine Bestätigung von Dynatrace über ein Verschulden oder eine Haftung in Bezug auf die Verletzung des Schutzes Personenbezogener Daten.

10. **Unterverarbeitung**

(a) Der Kunde erteilt seine allgemeine Genehmigung, Mitglieder der Dynatrace Group als Unterauftragsverarbeiter im Rahmen dieses AVV zu ernennen, und ermächtigt Dynatrace und Mitglieder der Dynatrace Group, weitere Unterauftragsverarbeiter zu beauftragen. Eine aktuelle Liste der aktuellen Unterauftragsverarbeiter für die Dynatrace-Angebote ist unter https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ zu finden. Um über neue Unterauftragsverarbeiter oder Änderungen bei Unterauftragsverarbeitern benachrichtigt zu werden, muss sich der Kunde unter https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ für die

Benachrichtigungen („**Datenschutzbenachrichtigungen**“) anmelden. Dynatrace wird die Liste der Unterauftragsverarbeiter mindestens dreißig (30) Tage vor dem Datum des Inkrafttretens der Änderung aktualisieren, um jede Hinzufügung oder Änderung von dritten Unterauftragsverarbeitern zu berücksichtigen. Kunden, die sich für den Erhalt von Aktualisierungen der Liste der Unterauftragsverarbeiter angemeldet haben, werden über die Änderung informiert.

(b) Soweit dies nach geltendem Datenschutzrecht erforderlich ist, kann der Kunde der Verarbeitung Personenbezogener Kundendaten durch einen neu ernannten Unterauftragsverarbeiter aus angemessenen Gründen in Bezug auf den Schutz Personenbezogener Kundendaten widersprechen und muss Dynatrace innerhalb von fünfzehn (15) Tagen nach Veröffentlichung der Benachrichtigung über die Änderungen auf der Liste der Unterauftragsverarbeiter schriftlich informieren, wobei die spezifischen Gründe für seinen Widerspruch anzugeben sind. Der Einwand des Kunden muss schriftlich erfolgen, wirtschaftlich vernünftig begründet sein und auf begründeten Bedenken hinsichtlich der Datenschutzpraktiken des vorgeschlagenen Unterauftragsverarbeiters beruhen. Nach einem Einwand werden die Parteien dann in gutem Glauben zusammenarbeiten, um die berechtigten Einwände des Kunden auszuräumen und den Wechsel des Unterauftragsverarbeiters vorzunehmen. Wenn innerhalb von fünfzehn (15) Tagen nach dem Einwand keine Einigung erzielt werden kann, kann Dynatrace nach eigenem Ermessen: (a) den Unterauftragsverarbeiter anweisen, die Personenbezogenen Kundendaten nicht zu verarbeiten, was zur Folge haben kann, dass eine Funktion der Dynatrace-Angebote ausgesetzt wird und dem Kunden nicht zur Verfügung steht, oder (b) der Kunde kann diesen AVV und die Vereinbarung sofort kündigen und Dynatrace erstattet umgehend einen anteiligen Teil der im Voraus bezahlten Gebühren für den Zeitraum nach dem Aussetzungs- oder Kündigungsdatum. Geht innerhalb der oben genannten Frist kein Widerspruch bei Dynatrace ein, so wird davon ausgegangen, dass der Kunde die Nutzung des neuen Unterauftragsverarbeiters genehmigt hat.

(c) Dynatrace muss: (i) mit jedem Unterauftragsverarbeiter einen schriftlichen Vertrag abschließen, der Datenschutzverpflichtungen enthält, die im Wesentlichen ähnliche angemessene vertragliche Verpflichtungen vorsehen, aber nicht weniger restriktiv sind als die in diesem AVV festgelegten, soweit dies für die Art der von diesem Unterauftragsverarbeiter erbrachten Dienstleistung angemessen ist; und (ii) für die Einhaltung der Verpflichtungen dieses AVV durch diesen Unterauftragsverarbeiter und für alle Handlungen oder Unterlassungen dieses Unterauftragsverarbeiters verantwortlich bleiben, die einen Verstoß von Dynatrace gegen seine Verpflichtungen aus diesem AVV verursachen.

**11. Löschung von Kundendaten bei Kündigung.** Nach Kündigung oder Ablauf der Vereinbarung werden Personenbezogene Kundendaten innerhalb von dreißig (30) Tagen gelöscht oder nach Wahl des Kunden zurückgegeben, es sei denn, sie müssen nach geltendem Recht aufbewahrt werden oder sind in Back-up-Systemen archiviert; in diesem Fall bleiben die Bestimmungen dieses AVV bestehen.

**12. Internationale Datenübermittlungen**

(a) Der Kunde ermächtigt Dynatrace und seine Unterauftragsverarbeiter, Personenbezogene Kundendaten über internationale Grenzen hinweg zu übertragen, einschließlich und ohne Einschränkung aus dem EWR, Vereinigten Königreich und/oder der Schweiz, Israel und China in die Vereinigten Staaten. Wenn Personenbezogene Kundendaten aus dem EWR oder der Schweiz in ein Land übermittelt werden, das nach geltendem Datenschutzrecht kein angemessenes Schutzniveau bietet („**eingeschränkte Übermittlung**“), vereinbaren die Parteien, dass die Übermittlung den Standardvertragsklauseln unterliegt, die hiermit durch Bezugnahme wie folgt in diesen AVV aufgenommen werden. Die Unterschriften auf diesem AVV oder der Vereinbarung stellen die Unterzeichnung der Standardvertragsklauseln und aller beigefügten Anhänge dar. Wenn die Übermittlung Personenbezogener Kundendaten vom Kunden („**Datenexporteur“)** an Dynatrace („**Datenimporteur**“) eine eingeschränkte Übermittlung ist und Datenschutzgesetze erfordern, dass ein gültiger Übermittlungsmechanismus eingerichtet wird, unterliegen die Übermittlungen den Standardvertragsklauseln.

(b) Die Standardvertragsklauseln werden wie folgt abgeschlossen:

i. Modul Zwei gilt (falls zutreffend);

ii. In Klausel 7 (Andocken) wird die optionale Andockklausel angewendet;

iii. In Klausel 8.5 und Klausel 16 (d) wird die Bestätigung der Löschung auf schriftliche Anfrage des Datenexporteurs bereitgestellt;

iv. In Klausel 8.9 wird das Prüfungsrecht gemäß Abschnitt 7 des AVV ausgeübt;

v. In Klausel 9 (Einsatz von Unterauftragsverarbeitern) gilt Option 2 „Allgemeine schriftliche Genehmigung“ für Unterauftragsverarbeiter und die Frist für die vorherige Benachrichtigung ist in Abschnitt 11 dieses AVV festgelegt;

vi. In Klausel 11 (Rechtsbehelf) ist die fakultative Formulierung nicht anwendbar;

vii. In Klausel 13 (Aufsicht) ist die zuständige Aufsichtsbehörde die Commission nationale de l’informatique et des libertes (CNIL).

viii. In Klausel 14 (f) und Klausel 16 (c) ist das Kündigungsrecht auf die Kündigung der Klauseln beschränkt;

ix. In Klausel 17 (Geltendes Recht) unterliegen die Standardvertragsklauseln französischem Recht;

x. In Klausel 18 (b) (Gerichtstand und Zuständigkeit) vereinbaren die Parteien, dass Streitigkeiten vor den Gerichten Frankreichs beigelegt werden;

xi. Anhang 1 der Standardvertragsklauseln muss mit den in Anhang A dieses AVV dargelegten Informationen ausgefüllt werden;

xii. Anhang 2 der Standardvertragsklauseln muss mit den in Anhang B dieses AVV dargelegten Informationen ausgefüllt werden; und

xiii. Eine neue Klausel 1 (e) wird zu den Standardvertragsklauseln hinzugefügt, die lautet wie folgt: „Soweit im Rahmen dieses AVV anwendbar, gelten diese Klauseln auch entsprechend für die Verarbeitung Personenbezogener Kundendaten durch die Parteien, die dem Schweizerischen Bundesgesetz über den Datenschutz unterliegen. Gegebenenfalls wird die Bezugnahme auf das Recht der EU-Mitgliedstaaten oder die EU-Aufsichtsbehörden so geändert, dass sie die entsprechende Bezugnahme nach schweizerischem Recht enthält, da sie sich auf die Übermittlung Personenbezogener Kundendaten bezieht, die dem Schweizerischen Bundesgesetz über den Datenschutz und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten als Aufsichtsbehörde im Rahmen dieser Klauseln unterliegen“.

(c) Soweit die Bereitstellung der Dynatrace-Angebote durch Dynatrace die Übermittlung von Personenbezogenen Kundendaten aus dem Vereinigten Königreich in ein Drittland beinhaltet, das nach den geltenden Gesetzen im Vereinigten Königreich kein angemessenes Schutzniveau für Personenbezogene Kundendaten bietet: (i) sind die Standardvertragsklauseln gemäß Abschnitt 13 zu verwenden und auszufüllen; (ii) wird den Standardvertragsklauseln eine neue Klausel 1(f) mit folgendem Wortlaut hinzugefügt: „Soweit anwendbar, gelten diese Klauseln, ergänzt durch Abschnitt 13, sinngemäß auch für die Verarbeitung Personenbezogener Kundendaten durch die Parteien, die den Datenschutzgesetzen des Vereinigten Königreichs unterliegen; und (iii) ist der UK-Nachtrag wie folgt zu ergänzen:

i. Tabelle 1 des UK-Nachtrags muss mit den Informationen in Anhang A ausgefüllt werden.

ii. Tabelle 2 des UK-Nachtrags muss mit den Informationen in Abschnitt 13 (c) dieses AVV ausgefüllt werden.

iii. Tabelle 3 des UK-Nachtrags ist wie folgt auszufüllen:

1) Die Liste der Parteien ist in Anhang A aufgeführt;

2) Eine Beschreibung der Übertragung ist in Anhang A dargelegt;

3) Eine Beschreibung der technischen und organisatorischen Maßnahmen ist in Anhang B dargelegt;

4) Die Liste der Unterauftragsverarbeiter befindet sich in Abschnitt 11 dieses AVV;

5) Zum Zwecke des Ausfüllens von Tabelle 4 des UK-Nachtrags können sowohl der Importeur als auch der Exporteur den UK-Nachtrag gemäß Abschnitt 19 des UK-Nachtrags beenden.

(d) Soweit Dynatraces Bereitstellung der Dynatrace-Angebote die Übermittlung Personenbezogener Kundendaten aus China in ein Drittland beinhaltet, das gemäß den geltenden Gesetzen in China nicht als ein angemessenes Schutzniveau für Personenbezogene Kundendaten eingestuft wurde, ist der Kunde dafür verantwortlich, alle folgenden Verpflichtungen für den Export Personenbezogener Kundendaten zu erfüllen (wenn der Kunde der Verantwortliche ist) oder sicherzustellen, dass alle folgenden Verpflichtungen von dem entsprechenden dritten Verantwortlichen erfüllt werden (wenn der Kunde der Auftragsverarbeiter ist):

i. Unterrichtung der Personen über den Namen und die Kontaktinformationen des Empfängers der Personenbezogenen Kundendaten im Ausland, den Zweck und die Mittel der Verarbeitung, die Kategorien der Personenbezogenen Kundendaten und die Methoden und Verfahren, mit denen die Personen bei dem Empfänger der Personenbezogenen Kundendaten im Ausland ihre Rechte geltend machen können;

ii. Sicherstellung einer rechtmäßigen Grundlage für den Export Personenbezogener Kundendaten und, wenn die Einwilligung der Personen die rechtmäßige Grundlage ist, Einholung einer separaten Einwilligung der Personen;

iii. Durchführung einer Folgenabschätzung des Schutzes Personenbezogener Daten für den Export Personenbezogener Kundendaten; und

iv. Ergreifung der im PIPL und den dazugehörigen Verwaltungsvorschriften vorgeschriebenen Schutzmaßnahmen (d. h. Bestehen der staatlichen Sicherheitsbewertung, Einreichung der ausgeführten Standardvertragsklauseln oder Erhalt der Zertifizierung), sofern keine Ausnahmeregelung gilt.

(e) Sollte eine Aufsichtsbehörde Standardvertragsklauseln oder ähnliche Datenübertragungsmechanismen einführen, aktualisieren oder ersetzen, behält sich Dynatrace das Recht vor, einen alternativen Compliance-Standard einzuführen, um die Standardvertragsklauseln oder den UK-Nachtrag für die rechtmäßige Übermittlung Personenbezogener Daten zu ersetzen oder zu ergänzen, oder neue Datenübertragungsmechanismen für andere Länder hinzuzufügen, sofern diese datenschutzrechtlich anerkannt sind. Dynatrace wird Kunden, die Datenschutzbenachrichtigungen abonnieren, dreißig (30) Tage im Voraus über die Annahme des alternativen Compliance-Standards informieren. Die Änderung gilt automatisch, wie in der Benachrichtigung von Dynatrace am Ende der Kündigungsfrist angegeben.

(f) Im Falle eines Widerspruchs oder einer Unstimmigkeit zwischen den nachstehenden Dokumenten gilt die folgende Rangfolge: (1) die Standardvertragsklauseln (der Auftragsverarbeiter kann jedoch nach Maßgabe von Abschnitt 11 dieses AVV Unterauftragsverarbeiter ernennen) oder ein ähnlicher Mechanismus, der nach den geltenden Datenschutzgesetzen speziell für internationale Datenübermittlungen erforderlich ist; (2) dieser AVV und (3) die Vereinbarung.

(g) Soweit Dynatrace Kundendaten übermittelt, die aus Brasilien stammen und durch das dort geltende Datenschutzrecht geschützt sind, wird Dynatrace die Grundsätze und Rechte der betroffenen Personen und die im LGPD vorgesehenen Datenschutzpflichten einhalten.

(h) Soweit Dynatrace Kundendaten übermittelt, die aus Japan stammen und durch das dort geltende Datenschutzrecht geschützt sind, wird Dynatrace die Grundsätze und Rechte der betroffenen Personen und die im APPI vorgesehenen Datenschutzpflichten einhalten.

(i) Soweit die Bereitstellung der Dynatrace-Angebote durch Dynatrace die Übertragung Personenbezogener Kundendaten aus Israel in ein Drittland beinhaltet, das gemäß den geltenden Gesetzen in Israel nicht als ein angemessenes Schutzniveau für Personenbezogene Kundendaten eingestuft wurde, ist der Kunde dafür verantwortlich, eine rechtmäßige Grundlage für den Export Personenbezogener Kundendaten zu gewährleisten. Zur Klarstellung: Dieser AVV stellt die schriftliche Verpflichtung von Dynatrace dar, die geeigneten Sicherheitsmaßnahmen zu ergreifen, die von den israelischen Datenschutzbestimmungen (Internationale Datenübertragung) von 2001 gefordert werden. Der Klarheit halber werden die Verpflichtungen in diesem DPA vom Kunden als ausreichend erachtet, um die Übertragung von

Informationen außerhalb Israels gemäß der Verordnung 3 der Datenschutzbestimmungen (Übertragung von Daten an Datenbanken außerhalb des Landes) von 2001 zu ermöglichen.

**13. Ergänzende spezifische Bedingungen für die Datenschutzgesetze der US-Bundesstaaten.**

(a) Die Definition von „geltende Datenschutzgesetze“ umfasst die Datenschutzgesetze der US-Bundesstaaten. „Datenschutzgesetze der US-Bundesstaaten“ bezeichnet alle staatlichen Gesetze in Bezug auf den Schutz und die Verarbeitung Personenbezogener Daten, die in den Vereinigten Staaten von Amerika in Kraft sind, einschließlich, aber nicht beschränkt auf den California Consumer Privacy Act in der geänderten Fassung gemäß California Privacy Rights Act („CCPA“), und ähnliche Datenschutzgesetze für Verbraucher in anderen US-Bundesstaaten, jeweils wie von Zeit zu Zeit geändert, ergänzt oder ersetzt.

(b) Wenn Dynatrace Personenbezogene Kundendaten verarbeitet, die den Datenschutzgesetzen der US-Bundesstaaten unterliegen, ist Dynatrace ein Dienstleister oder „Verarbeiter“ (wie jeweils anwendbar) bei der Verarbeitung Personenbezogener Kundendaten. Der Kunde legt Dynatrace die Personenbezogenen Kundendaten für einen begrenzten und spezifizierten Zweck offen oder stellt sie anderweitig zur Verfügung, um die Dynatrace-Angebote entsprechend der Vereinbarung bereitzustellen (der „Zweck“). Dynatrace verpflichtet sich (und verlangt Selbiges von Unterauftragsverarbeitern):

i. die für ihn als Dienstleister oder Verarbeiter im Rahmen der Datenschutzgesetze der US-Bundesstaaten geltenden Verpflichtungen zu erfüllen;

ii. mitzuteilen, wenn Dynatrace seinen Verpflichtungen aus den Datenschutzgesetzen der US-Bundesstaaten nicht mehr nachkommen kann;

iii. Kundeninhalte nicht zu „verkaufen“ oder „weiterzugeben“ (wie im CCPA definiert) oder Personenbezogene Kundendaten aufzubewahren, zu verwenden oder offenzulegen: (1) für einen anderen Zweck als den Zweck, einschließlich der Aufbewahrung, Verwendung oder Offenlegung Personenbezogener Kundendaten für einen anderen kommerziellen Zweck als den Zweck oder wie anderweitig durch die Datenschutzgesetze der US-Bundesstaaten erlaubt; oder (2) außerhalb der direkten Geschäftsbeziehung zwischen dem Kunden und Dynatrace; oder, sofern nicht anderweitig durch die Datenschutzgesetze der US-Bundesstaaten erlaubt, die Personenbezogenen Kundendaten nicht mit den Personenbezogenen Daten zu kombinieren, die Dynatrace von oder im Namen eines anderen Unternehmens oder einer anderen Person erhält oder die Dynatrace aus seinen eigenen Interaktionen mit Einzelpersonen erfasst, es sei denn, eine solche Kombination ist erforderlich, um einen Geschäftszweck zu erfüllen, der durch die Datenschutzgesetze der US-Bundesstaaten erlaubt ist.

iv. Der Kunde wird: (1) nach Benachrichtigung das Recht haben, angemessene und geeignete, von den Parteien vereinbarte Maßnahmen zu ergreifen, um dazu beizutragen, dass Dynatrace die Personenbezogenen Kundendaten in einer Weise verarbeitet, die mit den Verpflichtungen des Kunden gemäß den Datenschutzgesetzen der US-Bundesstaaten übereinstimmt, und um die unbefugte Verarbeitung Personenbezogener Kundendaten durch Dynatrace zu stoppen und zu beheben; (2) den Kunden benachrichtigen, wenn das Unternehmen feststellt, dass es seine Verpflichtungen als Dienstleister gemäß den Datenschutzgesetzen der US-Bundesstaaten nicht mehr erfüllen kann.

v. Dynatrace erkennt an und bestätigt, dass es keine Personenbezogenen Kundendaten als Gegenleistung für Angebote erhält, die dem Kunden bereitgestellt werden. Dynatrace bestätigt, dass es seine Verpflichtungen aus den Datenschutzgesetzen der US-Bundesstaaten zur Kenntnis genommen hat und einhalten wird.

**14. Sonstiges**

(a) Außer in der durch diesen AVV geänderten Fassung bleibt die Vereinbarung in vollem Umfang in Kraft und wirksam. Alle Änderungen an diesem AVV bedürfen der schriftlichen Unterzeichnung durch autorisierte Vertreter der Parteien.

(b) Ungeachtet anderslautender Bestimmungen in der Vereinbarung oder in diesem AVV unterliegt die Haftung jeder Partei und aller ihrer verbundenen Unternehmen insgesamt, die sich aus diesem AVV, einem Auftrag oder der Vereinbarung ergibt oder damit zusammenhängt, unabhängig davon, ob es sich um einen Vertrag, eine unerlaubte Handlung oder eine andere Haftungstheorie handelt, weiterhin dem Abschnitt „Haftungsbeschränkung“ der Vereinbarung, und jede Bezugnahme in diesem Abschnitt auf die Haftung einer Partei bedeutet die Gesamthaftung dieser Partei und aller ihrer verbundenen Unternehmen im Rahmen der Vereinbarung und dieses AVV, einschließlich aller Anhänge zu dieser Vereinbarung. Dynatrace haftet gegenüber dem Kunden nicht für indirekte oder Folgeschäden/-verluste, entgangenen Gewinn, Umsatzeinbußen, Geschäftseinbußen, entgangene Einsparungen, Verlust oder Beeinträchtigung des Firmenwerts oder sonstige direkte oder indirekte Schäden, die sich aus oder in Verbindung mit diesem AVV ergeben. Ohne die Verpflichtungen einer der Parteien aus der Vereinbarung oder diesem AVV einzuschränken, erklärt sich der Kunde damit einverstanden, dass jede Haftung, die Dynatrace in Bezug auf die Personenbezogenen Kundendaten entsteht, die sich aus der Nichteinhaltung der Verpflichtungen des Kunden aus diesem AVV oder dem anwendbaren Datenschutzgesetz ergibt, auf die Haftungsgrenze von Dynatrace aus der Vereinbarung (oder, falls zutreffend, aus diesem AVV) angerechnet wird und diese reduziert, als wäre es eine Haftung gegenüber dem Kunden. Ungeachtet anderslautender Bestimmungen in diesem AVV (einschließlich, aber nicht beschränkt auf die Entschädigungsverpflichtungen der Parteien) ist keine Partei für Geldbußen verantwortlich, die gemäß Artikel 83 der DSGVO von einer Aufsichtsbehörde oder staatlichen Stelle gegen die andere Partei im Zusammenhang mit einem Verstoß der anderen Partei gegen die DSGVO verhängt oder erhoben werden.

(c) Dieser AVV unterliegt den geltenden Gesetzen und den Bestimmungen der Gerichtsbarkeit in der Vereinbarung und wird in Übereinstimmung mit diesen ausgelegt, vorausgesetzt, dass die Standardvertragsklauseln gemäß Abschnitt 13 dieses AVV geregelt werden.

| | |
|---|---|
| Vereinbart und akzeptiert von: | Vereinbart und akzeptiert von: |
| **Kunde_Unternehmen_Name** | **Dynatrace_Unternehmen_Name** |
| Autorisierte Unterschrift | Autorisierte Unterschrift |
| Name | Name |
| Titel | Titel |
| Datum | Datum |
| Adresse | Adresse |
| Unternehmensnummer (falls zutreffend) | Unternehmensnummer (falls zutreffend) |

## Anhang A
## DETAILS DER VERARBEITUNG

**Beschreibung des Datenexporteurs**

Der Datenexporteur ist das Unternehmen, das in dem zwischen dem Datenexporteur und dem Datenimporteur bestehenden Auftragsverarbeitungsvertrag, dem dieser Anhang beigefügt ist, als „Kunde“ bzw. „Dynatrace“ im Falle einer Unterauftragsverarbeitung bezeichnet wird.

**Beschreibung des Datenimporteurs**

Der Datenimporteur ist das Unternehmen, das in dem zwischen dem Datenexporteur und dem Datenimporteur bestehenden Auftragsverarbeitungsvertrag, dem dieser Anhang beigefügt ist, als „Dynatrace“ oder ein ordnungsgemäß autorisierter Unterauftragsverarbeiter bezeichnet wird.

**Gegenstand und Dauer der Verarbeitung**

Gegenstand und Dauer der Verarbeitung sind wie folgt:

Im Verhältnis zwischen den Parteien ist der Kunde der Verantwortliche für bestimmte Personenbezogene Kundendaten, die Dynatrace vom Kunden in Verbindung mit seiner Nutzung von Dynatrace-Angeboten bereitgestellt werden. Die Dauer der Verarbeitung ist die Laufzeit der Vereinbarung.

**Zwecke der Verarbeitung**

Die Verarbeitung ist für folgende Zwecke erforderlich:

Um Dynatrace zu ermöglichen, dem Kunden die Dynatrace-Angebote bereitzustellen und seine Rechte und Pflichten aus der Vereinbarung auszuüben.

**Betroffene Personen**

Zu den betroffenen Personen können folgende Parteien gehören: (i) Benutzer, die vom Kunden autorisiert wurden, die Dynatrace-Angebote zu nutzen, und (ii) Benutzer oder Besucher der überwachten Anwendungen und/oder Websites des Kunden (einschließlich, aber nicht beschränkt auf die Mitarbeiter, Kunden oder Klienten, Vertreter, Auftragnehmer und Berater des Kunden), wie vom Kunden nach eigenem Ermessen festgelegt.

**Art der Personenbezogenen Daten**

Der Kunde muss bestimmte Personenbezogene Daten angeben, um die Dynatrace-Angebote nutzen zu können, einschließlich der IP-Adresse und des Vor- und Nachnamens, falls dieser in der E-Mail-Adresse und den Benutzeranmeldeinformationen eines Benutzers enthalten ist. Der Kunde kann zusätzliche Personenbezogene Daten an die Dynatrace-Angebote übermitteln, deren Umfang vom Kunden nach eigenem Ermessen festgelegt und kontrolliert wird.

**Besondere Kategorien von Daten oder sensible Personenbezogene Daten (falls zutreffend)**

Die übermittelten Personenbezogenen Daten betreffen die folgenden besonderen Kategorien von Daten oder sensible Personenbezogene Daten:

Nicht zutreffend. Der Kunde darf die Dynatrace-Angebote nicht verwenden, um Daten zu verarbeiten, die als „Daten besonderer Kategorien“ oder „sensible personenbezogene Daten“ klassifiziert sind, es sei denn, dies wurde ausdrücklich schriftlich vereinbart.

**Verarbeitungsvorgänge**

Die übermittelten Personenbezogenen Daten unterliegen den folgenden grundlegenden Verarbeitungstätigkeiten:

Dynatrace verarbeitet die Personenbezogenen Kundendaten nur, soweit dies zur Bereitstellung der Dynatrace-Angebote und zur Ausübung seiner Rechte und Pflichten gemäß den Bedingungen der Vereinbarung und dieses Auftragsverarbeitungsvertrags erforderlich ist, einschließlich, aber nicht beschränkt auf Kundeneinbeziehung, technischen Support, professionelle Dienstleistungen, Verbesserung der Leistung und Funktionen von Dynatrace-Angeboten, Benutzerauthentifizierung, Kommunikation und Kontoverwaltung.

## Anhang B

## SICHERHEITSMASSNAHMEN

Dynatrace (hierin auch als der „Auftragsverarbeiter“ bezeichnet) setzt in Bezug auf die Kundendaten, die es im Auftrag des Kunden (hierin auch als „Verantwortlicher bezeichnet“) verarbeitet, mindestens die nachstehend beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen um. Diese Sicherheitsmaßnahmen müssen auf alle Personenbezogenen Kundendaten angewendet werden, die der zugrundeliegenden Vereinbarung zwischen dem Auftragsverarbeiter und dem Datenverantwortlichen (die „Vereinbarung“) unterliegen. In Bezug auf dritte Unterauftragsverarbeiter, die Personenbezogene Daten im Auftrag von Dynatrace verarbeiten können, hat dieser Dritte seine eigenen Sicherheitsanforderungen zum Schutz der Personenbezogenen Daten.

### Technische Maßnahmen

1.1 Autorisierung

(a) Ein Autorisierungssystem wird verwendet, wenn verschiedene Autorisierungsprofile für verschiedene Zwecke verwendet werden.

1.2 Identifikation

(a) Jedem befugten Benutzer muss ein persönlicher und eindeutiger Identifikationscode für diesen Zweck ausgestellt werden („Benutzer-ID“). Eine Benutzer-ID darf keiner anderen Person zugewiesen werden, nicht einmal zu einem späteren Zeitpunkt.

(b) Ein aktueller Datensatz über befugte Benutzer und den ihnen jeweils zur Verfügung stehenden Zugriff muss gepflegt werden und es müssen Zugriffs- und Authentifizierungsverfahren für jeglichen Zugriff auf Informationssysteme oder für die Durchführung von Datenverarbeitung eingerichtet werden. Wie hierin verwendet, bezieht sich „Verarbeitung“ auf Tätigkeiten oder eine Reihe an Tätigkeiten, die bezüglich Daten ausgeführt werden, ob mit oder ohne automatische Mittel, wie etwa die Erfassung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung, das Abrufen, die Beratung, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder das anderweitige Verfügbarmachen, Abgleichen oder Kombinieren, die Beschränkung, Löschung oder Vernichtung.

(c) Passwörter müssen, wie in den Richtlinien zur Informationssicherheit festgelegt, regelmäßig geändert werden.

1.3 Authentifizierung

(a) Befugte Benutzer dürfen Daten verarbeiten, wenn ihnen Authentifizierungsdaten bereitgestellt werden, wie zum Beispiel zum erfolgreichen Abschluss eines Authentifizierungsverfahrens, das sich entweder auf eine bestimmte Verarbeitungstätigkeit oder eine Reihe an Verarbeitungstätigkeiten bezieht.

(b) Die Authentifizierung muss auf einem geheimen Passwort basieren, das mit der Benutzer-ID verknüpft ist, und welches nur dem befugten Benutzer bekannt ist.

(c) Ein oder mehrere Authentifizierungsdatensätze müssen einem befugten Benutzer zugewiesen oder mit ihm verknüpft werden.

(d) Es muss ein Verfahren zur Vertraulichkeit und Integrität des Passworts durchgeführt werden. Passwörter müssen so gespeichert werden, dass sie während ihrer Gültigkeit nicht verständlich

sind. Es muss ein Verfahren zum Zuweisen, Verteilen und Speichern von Passwörtern geben.

(e) Passwörter müssen mindestens zwölf Zeichen umfassen oder, wenn dies technisch aufgrund der entsprechenden Informationssysteme nicht erlaubt ist, muss ein Passwort aus der maximal zulässigen Anzahl von Zeichen bestehen. Passwörter dürfen keine Zeichen enthalten, die leicht mit dem befugten Benutzer, der für die Verarbeitung zuständig ist, verknüpft werden können und müssen in regelmäßigen Abständen, welche im Sicherheitsdokument festgelegt werden müssen, geändert werden. Passwörter müssen, wenn sie erstmalig verwendet werden und danach regelmäßig vom befugten Benutzer auf einen geheimen Wert geändert werden, der nur dem befugten Benutzer bekannt ist.

(f) Zusätzlich zu einer gültigen Kombination aus Benutzer-ID und Passwort muss jeder Zugriff auf Dynatrace-Daten oder -Systeme durch eine Multi-Faktor-Authentifizierung („MFA“) gesichert werden. Bei der MFA-Lösung kann es sich entweder um Software oder Hardware handeln.

(g) Authentifizierungsdaten müssen ebenfalls deaktiviert werden, wenn dem befugten Benutzer gekündigt wird, er versetzt wird oder ihm der Zugriff auf die Informationssysteme oder Verarbeitungsdaten entzogen wird.

1.4 Zugriffskontrollen

(a) Nur befugte Benutzer haben Zugriff auf Daten, einschließlich bei Speicherung auf elektronischen oder Wechselmedien oder wenn sie übertragen werden. Befugte Benutzer haben nur für die Daten und Ressourcen Zugriffsrechte, die für diese erforderlich sind, um ihre Pflichten auszuführen.

(b) Ein System zur Gewährung des Zugriffs für befugte Benutzer auf bestimmte Daten und Ressourcen wird verwendet.

(c) Es wird halbjährlich überprüft, ob die Voraussetzungen für die Bewahrung der relevanten Genehmigungsprofile weiterhin gelten. Dies kann auch eine Liste an befugten Benutzer beinhalten, die mittels homogener Aufgabenkategorien und dem entsprechenden Autorisierungsprofil erstellt wird.

(d) Es müssen Maßnahmen ergriffen werden, um zu verhindern, dass ein Benutzer unbefugten Zugriff auf die Informationssysteme erhält oder sie in unbefugter Weise nutzt. Insbesondere sollten Angriffserkennungssysteme (Intrusion-Detection-Systeme), die die branchenübliche gute Praxis reflektieren, installiert werden, um die Informationssysteme vor unbefugtem Zugriff zu schützen.

(e) Die Betriebssystem- oder Datenbankzugriffskontrollen müssen korrekt konfiguriert werden, um sicherzustellen, dass nur befugter Zugriff möglich ist.

(f) Nur befugte Mitarbeiter dürfen den Zugriff auf die Informationssysteme gewähren, ändern oder stornieren.

1.5 Verwaltung von Computersystemen und Wechselmedien

(a) Netzwerkinformationssysteme und physische Medien, die Daten speichern, müssen in einer sicheren Umgebung mit physischem Zugriff aufbewahrt und auf Mitarbeiter beschränkt werden, die ein Zugriffsrecht haben. Eine strenge Genehmigungs- und Zugriffskontrolle muss gepflegt werden.

(b) Die Software, Firmware und Hardware, die in den Informationssystemen verwendet werden, muss jährlich überprüft werden, um Schwachstellen und Mängel in den Informationssystemen zu erkennen und solche Schwachstellen und Mängel zu beheben.

(c) Es werden Richtlinien und Schulungen zur Aufbewahrung und Verwendung von Datenträgern, auf denen Daten gespeichert sind, herausgegeben, um unbefugten Zugriff und Verarbeitung zu

verhindern.

(d) Wenn Datenträger entsorgt oder wiederverwendet werden sollen, sind die erforderlichen Maßnahmen zu treffen, um zu verhindern, dass die zuvor auf ihnen gespeicherten Daten und sonstigen Informationen zu einem späteren Zeitpunkt abgerufen werden können, oder um die Informationen auf andere Weise lesbar zu machen oder durch technische Mittel zu rekonstruieren, bevor sie aus dem Bestand genommen werden. Alle wiederverwendbaren Medien, die für die Speicherung von Daten verwendet werden, werden vor der Entsorgung oder Wiederverwendung mindestens drei Mal mit randomisierten Daten überschrieben.

(e) Die Entfernung von Medien, die Daten von den dedizierten Räumlichkeiten enthalten, muss vom Datenverantwortlichen und in Übereinstimmung mit den Dynatrace-Richtlinien konkret genehmigt werden.

(f) Medien, die Daten enthalten, müssen gelöscht oder unleserlich gemacht werden, wenn sie nicht mehr verwendet werden, sowie vor der ordnungsgemäßen Entsorgung.

1.6 Verteilung oder Übermittlung

(a) Daten dürfen nur befugten Benutzern zur Verfügung stehen.

(b) Verschlüsselung (128-Bit oder stärker) oder eine andere gleichwertige Form des Schutzes muss zum Schutz von Daten verwendet werden, die elektronisch über ein öffentliches Netzwerk übermittelt oder auf einem tragbaren Gerät gespeichert werden, oder wo es erforderlich ist, Daten in einer physisch unsicheren Umgebung zu speichern oder zu verarbeiten.

(c) Wenn Daten die dedizierten Räumlichkeiten als Folge der Wartungsvorgänge verlassen, müssen die notwendigen Maßnahmen ergriffen werden, um die unbefugte Rücknahme der Daten und anderen darin gespeicherten Informationen zu verhindern.

(d) Wenn Daten übertragen oder über ein elektronisches Kommunikationsnetzwerk übermittelt werden, müssen Maßnahmen ergriffen werden, um den Datenfluss zu steuern und den Zeitpunkt der Übertragung oder Übermittlung, die übertragenen oder übermittelten Daten, den Zielort der übertragenen oder übermittelten Daten und Details zum befugten Benutzer, der die Übertragung oder Übermittlung durchführt, aufzuzeichnen.

1.7 Erhaltung, Backup-Kopien und Wiederherstellung

(a) Verfahren für die Erstellung von Back-up-Kopien und zur Wiederherstellung von Daten müssen definiert und festgelegt werden. Diese Verfahren müssen den Zustand der Daten wiederherstellen, in dem sie sich zum Zeitpunkt ihres Verlusts oder ihrer Zerstörung befanden.

(b) Back-up-Kopien müssen mindestens einmal wöchentlich erstellt werden, es sei denn, es wurden zu dieser Zeit keine Daten aktualisiert.

(c) Eine Back-up-Kopie und Datenwiederherstellungsverfahren müssen an verschiedenen Standorten des Ortes der Informationssysteme aufbewahrt werden, die Daten verarbeiten, und diese Mindestsicherheitsanforderungen gelten für solche Back-up-Kopien.

1.8 Anti-Virus und Intrusion Detection

(a) Anti-Virus-Software und Intrusion-Detection-Systeme sollten auf Informationssystemen installiert werden, um sich vor Angriffen oder anderen unbefugten Handlungen im Hinblick auf Informationssysteme zu schützen. Anti-Virus-Software und Intrusion-Detection-Systeme sollten regelmäßig entsprechend der branchenüblichen guten Praxis für die betroffenen Informationssysteme (und mindestens einmal jährlich) aktualisiert werden.

1.9 Tests

(a) Tests vor der Implementierung oder Änderung der Informationssysteme, die Daten verarbeiten, dürfen keine echten oder „Live“-Daten verwenden, es sei denn, diese Verwendung ist notwendig und es gibt keine angemessene Alternative. Wenn echte oder „Live“-Daten verwendet werden, wird dies auf den Umfang beschränkt, der für die Testverfahren und die Sicherheitsstufe, die dem Typ der verarbeiteten Daten entspricht, notwendig ist.

1.10 Prüfung

(a) Regelmäßige Prüfungen der Einhaltung dieser Sicherheitsanforderungen müssen mindestens einmal jährlich durchgeführt werden.

(b) Die Ergebnisse müssen eine Stellungnahme zum Umfang abgeben, in dem die angenommenen Sicherheitsmaßnahmen und Kontrollen diese Sicherheitsanforderungen einhalten, etwaige Defizite identifizieren und ggf. Korrekturmaßnahmen oder ergänzende Maßnahmen vorschlagen. Sie sollten auch die Daten, Fakten und Beobachtungen, die zu der Meinung geführt haben, und die vorgeschlagenen Empfehlungen beinhalten.

**2. Organisatorische Maßnahmen**

2.1 Sicherheitsplan und -dokument

- Die Maßnahmen, die zur Einhaltung dieser Sicherheitsanforderungen ergriffen wurden, sind der Gegenstand der Richtlinien zur Informationssicherheit des Unternehmens und werden in einem Sicherheitsportal festgelegt, das auf dem neuesten Stand gehalten und überarbeitet wird, wenn relevante Änderungen am/an den Informationssystem(en) oder den technischen oder organisatorischen Maßnahmen vorgenommen werden.
- Die Richtlinien zur Informationssicherheit behandeln Folgendes:

  (i) Sicherheitsmaßnahmen im Zusammenhang mit der Änderung und Wartung des/der Systems/Systeme, das/die zur Verarbeitung von Daten verwendet werden, einschließlich Entwicklung und Wartung von Anwendungen, angemessener Anbieterunterstützung und Bestand an Hardware und Software;

  (ii) Physische Sicherheit, einschließlich Sicherheit der Gebäude oder Räumlichkeiten, in denen Datenverarbeitung stattfindet, Sicherheit von Datenausrüstung, Telekommunikationsinfrastruktur und Umweltkontrollen; und

  (iii) Sicherheit von Computern und Telekommunikationssystemen, einschließlich Verfahren zur Verwaltung von Back-up-Kopien, Verfahren zum Umgang mit Computerviren, Verfahren zum Verwalten von Signalen/Codes, Sicherheit für die Software-Implementierung, Sicherheit im Zusammenhang mit Datenbanken, Sicherheit für die Verbindung von Systemen mit dem Internet, Überprüfung der Umgehung von Datensystemen, Mechanismen zur Erfassung von Versuchen, die Systemsicherheit zu durchbrechen oder sich unbefugten Zugang zu verschaffen.

- Der Sicherheitsplan umfasst alle Dynatrace-Richtlinien, die von Zeit zu Zeit aktualisiert werden, einschließlich unter anderem:

  (i) den Verhaltens- und Ethikkodex

  (ii) die Globale Datenschutzrichtlinie

  (iii) die Dynatrace IT-Richtlinie zur akzeptablen Nutzung

  (iv) System-Sicherheitsrichtlinien: Dynatrace-Richtlinie zur Verwaltung der Zugangskontrolle; Standard zur Aufbewahrung von Backups; Richtlinie zum Änderungsmanagement; Richtlinie zum Änderungsmanagement – Geschäftssysteme; Compliance-Richtlinie; Reaktionsplan für Cyber- und Datensicherheitsvorfälle; Richtlinie zur Datenklassifizierung; Richtlinie zur

Verhinderung von Datenverlust; Richtlinie zur elektronischen Überwachung; Verschlüsselungsrichtlinie; Sicherheitsrichtlinie der Personalabteilung; Richtlinie zur Verwaltung von Informationsressourcen; Richtlinie zum Informationsrisikomanagement; Richtlinie zum IT-Betrieb; Richtlinie zu mobilen Geräten; Richtlinie zum Netzwerkzugriff; Passwortrichtlinie für Netzwerkkonten; Richtlinie zur Netzwerk-Firewall; Richtlinie für physische Sicherheit und Umwelt; Richtlinie zur Rückgabe von Vermögenswerten für gekündigte Mitarbeiter; Secure; Sicherheits-Phishing-Richtlinie; Richtlinie zum Lebenszyklus von Servicekonten; Richtlinie zum Lieferantenmanagement; Richtlinie zum Schwachstellenmanagement; Richtlinie für Sicherheit am Arbeitsplatz.

(v) Der Sicherheitsplan ist Mitarbeitern zugänglich, die Zugriff auf Daten und Informationssysteme haben und muss mindestens die folgenden Aspekte abdecken:

(vi) Den Umfang mit einer detaillierten Spezifikation geschützter Ressourcen;

(vii) Die Maßnahmen, Standards, Verfahren, Verhaltensregeln und Normen zur Gewährleistung der Sicherheit, einschließlich der Kontrolle, Inspektion und Überwachung der Informationssysteme;

(viii) Die Verfahren zum Melden, Verwalten und Reagieren auf Vorfälle; und

(ix) Die Verfahren für die Erstellung von Sicherungskopien und die Wiederherstellung von Daten, einschließlich des Mitarbeiters, der die Verarbeitungstätigkeit durchgeführt hat; die wiederhergestellten Daten und gegebenenfalls die Daten, die manuell in den Wiederherstellungsprozess eingegeben werden mussten.

2.2 Funktionen und Pflichten von Mitarbeitern

- Nur Mitarbeiter, die ein legitimes Betriebsbedürfnis haben, um auf die Informationssysteme zuzugreifen oder die Datenverarbeitung durchzuführen, dürfen dazu befugt werden („**befugte Benutzer**").

- Die notwendigen Maßnahmen sind zu ergreifen, um die Mitarbeiter mit diesen Mindestsicherheitsanforderungen, relevanten Richtlinien und geltenden Gesetzen hinsichtlich der Erfüllung ihrer Funktionen und Pflichten bezüglich der Verarbeitung von Daten und den Folgen der Verletzung dieser Anforderungen vertraut zu machen und sie darin zu schulen.
- Die Funktionen und Pflichten der Mitarbeiter, die Zugriff auf Daten haben, müssen über die Rollen der Anwendungssicherheitsrollen klar definiert werden.
- Befugte Benutzer müssen angewiesen werden, dass elektronische Geräte nicht unbeaufsichtigt gelassen werden oder während der Verarbeitung zugänglich gemacht werden dürfen. Der physische Zugriff auf Bereiche, in denen Daten gespeichert werden, ist auf befugte Benutzer beschränkt. Die Disziplinarmaßnahmen für einen Verstoß gegen den Sicherheitsplan müssen klar definiert, dokumentiert und dem Personal mitgeteilt werden.

2.3 Chief Security Officer

- Eine oder mehrere Person(en), die für die Gesamteinhaltung dieser Mindestanforderungen verantwortlich ist/sind, muss/müssen als Chief Security Officer („**CISO**") benannt werden. Der CISO muss angemessen ausgebildet und in der Verwaltung von Informationssicherheit geschult werden und verfügt über entsprechende Ressourcen, um die Einhaltung effektiv zu gewährleisten.
- Die Kontaktdaten des CISO werden dem Datenverantwortlichen auf Anfrage bereitgestellt.

2.4 Aufzeichnungen

- Ein Verlauf des befugten Zugriffs oder der Offenlegung von Daten muss mit einem sicheren Prüfpfad aufgezeichnet werden.
- Nur die Mitarbeiter, die ordnungsgemäß befugt sind, dürfen physischen Zugriff auf die Räumlichkeiten haben, in denen Informationssysteme und Medien mit Daten aufbewahrt werden.
- Es gibt ein Verfahren zur Meldung, Reaktion und Verwaltung von Sicherheitsvorfällen wie Datensicherheitsverletzungen. Dies muss mindestens Folgendes umfassen:
  - (i) Ein Verfahren zur Meldung solcher Vorfälle/Verstöße an das entsprechende Management;
  - (ii) Ein klar bezeichnetes Team zur Verwaltung und Koordinierung der Reaktion auf einen Vorfall, das vom CISO geführt wird;
  - (iii) Einen dokumentierten Prozess für die Verwaltung der Reaktion auf einen Vorfall, einschließlich der Anforderung, angemessene Probleme und Maßnahmenprotokolle zu aufzuzeichnen, um dem Zeitpunkt zu berücksichtigen, zu dem der Vorfall stattgefunden hat, die Person, die ihn gemeldet hat, und die Auswirkungen davon;
  - (iv) Die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen unverzüglich zu benachrichtigen, wenn eine Sicherheitsverletzung vorliegt, die zur versehentlichen oder unrechtmäßigen Vernichtung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf vom Auftragsverarbeiter übermittelte, gespeicherte oder anderweitig verarbeitete Daten führt; und
  - (v) Das Sicherheits-/Vorfallmanagement-Team des Auftragsverarbeiters sollte gegebenenfalls zusammen mit den Sicherheitsvertretern des Datenverantwortlichen zusammenarbeiten, bis der Vorfall oder die Verletzung zufriedenstellend behoben wurde.
  - (vi) Das Verfahren zur Meldung, Verwaltung und Reaktion auf Vorfälle muss mindestens einmal jährlich getestet werden.