Artikel I, Geschäftsbezogene Kontaktinformationen

Dieser Artikel gilt, wenn der Lieferant oder Kyndryl geschäftsbezogene Kontaktinformationen des anderen verarbeitet.

1.1 Kyndryl und der Lieferant können die geschäftsbezogenen Kontaktinformationen des anderen in Verbindung mit der Bereitstellung von Leistungen und Waren verarbeiten, wo sie geschäftlich tätig sind.

1.2 Eine Partei:

a) wird die geschäftsbezogenen Kontaktinformationen der anderen Partei nicht für andere Zwecke verwenden oder offenlegen (genauer gesagt, wird keine Partei die geschäftsbezogenen Kontaktinformationen der anderen Partei verkaufen oder die geschäftsbezogenen Kontaktinformationen der anderen Partei ohne deren vorherige schriftliche Zustimmung und ggf. der betroffenen Personen für Marketingzwecke verwenden oder offenlegen) und

b) wird umgehend auf schriftliche Anforderung der anderen Partei Informationen über die Verarbeitung der geschäftsbezogenen Kontaktinformationen der anderen Partei löschen, ändern, berichtigen, zurückgeben und bereitstellen, deren Verarbeitung beschränken oder sonstige in angemessenem Rahmen geforderte Maßnahmen in Verbindung damit ergreifen.

1.3 Die Parteien gehen keine gemeinsame Beziehung als Verantwortliche in Bezug auf die geschäftsbezogenen Kontaktinformationen der anderen Partei ein, ferner wird keine im Auftragsdokument enthaltene Bestimmung als Hinweis auf die Absicht, eine gemeinsame Beziehung als Verantwortliche zu etablieren, interpretiert oder ausgelegt.

1.4 Die Kyndryl Datenschutzerklärung unter https://www.kyndryl.com/privacy enthält zusätzliche Informationen über die Verarbeitung geschäftsbezogener Kontaktinformationen durch Kyndryl.

1.5 Die Parteien haben technische und organisatorische Sicherheitsmaßnahmen zum Schutz der geschäftsbezogenen Kontaktinformationen der anderen Partei vor Verlust, Vernichtung, Veränderung, versehentlicher oder nicht autorisierter Offenlegung, versehentlichem oder unbefugtem Zugriff und rechtswidriger Verarbeitung implementiert und werden diese aufrechterhalten.

1.6 Der Lieferant wird Kyndryl umgehend (jedoch spätestens innerhalb von 48 Stunden) benachrichtigen, wenn er Kenntnis über eine Sicherheitsverletzung erlangt, die geschäftsbezogene Kontaktinformationen von Kyndryl betrifft. Diese Benachrichtigung erfolgt über das Kyndryl Global Procurement-Support-Portal unter https://www.kyndryl.com/procurement/procSupport. Der Lieferant wird Kyndryl auf Anforderung in angemessenem Umfang Informationen über eine solche Sicherheitsverletzung und den Status seiner Abhilfe- und Wiederherstellungsmaßnahmen bereitstellen. In angemessenem Rahmen geforderte Informationen können beispielsweise Protokolle enthalten, die berechtigten, administrativen und sonstigen Zugriff auf Geräte, Systeme oder Anwendungen, forensische Abbildungen von Geräten, Systemen oder Anwendungen und andere vergleichbare Elemente nachweisen, sofern dies für die Sicherheitsverletzung oder die Abhilfe- und Wiederherstellungsmaßnahmen des Lieferanten relevant ist.

1.7 Wenn der Lieferant die geschäftsbezogenen Kontaktinformationen von Kyndryl nur verarbeitet und keinen Zugriff auf andere Daten oder Materialien oder auf Kyndryl Unternehmenssysteme hat, sind dieser Artikel und Artikel X (Mitwirkung, Überprüfung und Fehlerbehebung) die einzigen Artikel, die für diese Verarbeitung Anwendung finden.

Artikel II, Technische und organisatorische Maßnahmen, Datensicherheit

Dieser Artikel gilt, wenn der Lieferant Kyndryl Daten verarbeitet, bei denen es sich nicht um geschäftsbezogene Kontaktinformationen von Kyndryl handelt. Der Lieferant wird bei der Bereitstellung aller Leistungen und Waren die Anforderungen dieses Artikels einhalten und dabei Kyndryl Daten vor Verlust, Vernichtung, Veränderung, versehentlicher oder nicht autorisierter Offenlegung, versehentlichem oder unbefugtem Zugriff und rechtswidriger Verarbeitung schützen. Die Anforderungen dieses Artikels erstrecken sich auf alle IT-Anwendungen, -Plattformen und -Infrastrukturen, die der Lieferant im Rahmen der Bereitstellung von Waren und Leistungen betreibt oder verwaltet, einschließlich aller Entwicklungs-, Test-, Hosting-, Support-, Betriebs- und Rechenzentrumsumgebungen.

1. Nutzung von Daten

1.1. Der Lieferant darf den Kyndryl Daten, ohne vorherige schriftliche Zustimmung von Kyndryl, keine sonstigen Informationen oder Daten, einschließlich personenbezogener Daten, hinzufügen oder darin einschließen. Ferner darf der Lieferant keine Kyndryl Daten in irgendeiner Form, weder aggregiert noch anderweitig, für andere Zwecke außer zur Bereitstellung von Leistungen und Waren verwenden (zum Beispiel ist es dem Lieferanten nicht gestattet, Kyndryl Daten zur Bewertung der Effektivität oder der Mittel zur Verbesserung seiner Angebote, für Forschung und Entwicklung zur Schaffung neuer Angebote oder zur Erstellung von Berichten über seine Angebote zu verwenden oder wiederzuverwenden). Sofern im Auftragsdokument nicht ausdrücklich gestattet, darf der Lieferant Kyndryl Daten nicht verkaufen.

1.2. Der Lieferant wird keine Web-Tracking-Technologien in die Waren oder Leistungen integrieren (diese Technologien umfassen HTML5, lokalen Speicher, Tags oder Token Dritter und Web-Beacons), es sei denn, dies ist im Auftragsdokument ausdrücklich gestattet.

2. Anforderungen Dritter und Vertraulichkeit

2.1. Der Lieferant verpflichtet sich, Kyndryl Daten nicht gegenüber Dritten offenzulegen, es sei denn, es liegt eine schriftliche Genehmigung von Kyndryl vor. Falls eine Regierungsbehörde, z. B. eine Regulierungsbehörde, Zugriff auf Kyndryl Daten anfordert (z. B. wenn die US-Regierung gegen den Lieferanten eine Anordnung zur nationalen Sicherheit (National Security Order) erlässt, um Kyndryl Daten zu erhalten), oder falls eine Offenlegung von Kyndryl Daten anderweitig gesetzlich vorgeschrieben ist, wird der Lieferant Kyndryl schriftlich über eine solche Anforderung oder Vorschrift benachrichtigen und Kyndryl die Gelegenheit geben, eine Offenlegung anzufechten (sofern eine Benachrichtigung gesetzlich untersagt ist, wird der Lieferant geeignete Schritte einleiten, um diese Untersagung und die Offenlegung von Kyndryl Daten rechtlich oder anderweitig anzufechten).

2.2. Der Lieferant versichert Kyndryl, dass (a) nur die Mitarbeiter, die für die Bereitstellung von Leistungen oder Waren Zugriff auf Kyndryl Daten benötigen, diesen Zugriff erhalten und nur in dem Umfang, der für die Bereitstellung dieser Leistungen und Waren erforderlich ist, und (b) seine Mitarbeiter an Geheimhaltungsverpflichtungen gebunden sind, die eine Verwendung und Offenlegung von Kyndryl Daten nur in Übereinstimmung mit diesen Bedingungen gestatten.

3. Rückgabe oder Löschung von Kyndryl Daten

3.1. Der Lieferant wird nach Wahl von Kyndryl Kyndryl Daten bei Kündigung oder Ablauf des Auftragsdokuments oder auf Anforderung von Kyndryl auch zu einem früheren Zeitpunkt entweder löschen oder zurückgeben. Falls Kyndryl die Löschung anfordert, wird der Lieferant die Daten in Übereinstimmung mit branchenüblichen Best Practices unlesbar machen, dafür sorgen, dass die Daten nicht erneut assembliert oder wiederhergestellt werden können, und die Löschung gegenüber Kyndryl nachweisen. Sollte Kyndryl die Rückgabe von Kyndryl Daten anfordern, wird der Lieferant dies in Übereinstimmung mit einer angemessenen Terminplanung und angemessenen schriftlichen Weisungen von Kyndryl tun.

Artikel III, Datenschutz

Dieser Artikel gilt, wenn der Lieferant personenbezogene Daten von Kyndryl verarbeitet.

1. Verarbeitung

1.1 Kyndryl ernennt den Lieferanten als Auftragsverarbeiter für die Verarbeitung personenbezogener Daten von Kyndryl zum alleinigen Zweck der Bereitstellung der Waren und Leistungen in Übereinstimmung mit den Weisungen von Kyndryl, einschließlich der in diesen Bedingungen, im Auftragsdokument und in der zugehörigen Rahmenvereinbarung zwischen den Parteien enthaltenen Weisungen. Sollte der Lieferant eine Weisung nicht einhalten, kann Kyndryl den betroffenen Teil der Leistungen durch schriftliche Benachrichtigung des Lieferanten kündigen. Ist der Lieferant der Auffassung, dass eine Weisung gegen ein Datenschutzgesetz verstößt, wird der Lieferant Kyndryl unverzüglich und innerhalb des gesetzlich geforderten Zeitrahmens darüber informieren.

1.2 Der Lieferant verpflichtet sich zur Einhaltung aller für die Leistungen und Waren geltenden Datenschutzgesetze.

1.3 In einem Anhang zum Auftragsdokument oder im Auftragsdokument selbst ist Folgendes in Bezug auf Kyndryl Daten festgelegt:

(a) Kategorien betroffener Personen;
(b) Arten personenbezogener Daten von Kyndryl;
(c) Datenaktionen und Verarbeitungstätigkeiten;
(d) Dauer und Häufigkeit der Verarbeitung; und
(e) eine Liste der Unterauftragsverarbeiter.

2. Technische und organisatorische Maßnahmen

2.1 Der Lieferant verpflichtet sich, die in Artikel II (Technische und organisatorische Maßnahmen, Datensicherheit) und Artikel VIII (Technische und organisatorische Maßnahmen, allgemeine Sicherheit) aufgeführten technischen und organisatorischen Maßnahmen zu implementieren und aufrechtzuerhalten und damit ein dem Risiko seiner Leistungen und Waren angemessenes Schutzniveau zu gewährleisten. Der Lieferant bestätigt, dass er die Einschränkungen in Artikel II, diesem Artikel III und Artikel VIII verstanden hat und einhalten wird.

3. Rechte und Anträge betroffener Personen

3.1 Der Lieferant wird Kyndryl unverzüglich (nach einem Zeitplan, der es Kyndryl und sonstigen Verantwortlichen ermöglicht, ihre gesetzlichen Verpflichtungen einzuhalten) über Anträge von betroffenen Personen, ihre Betroffenenrechte (z. B. Berichtigung, Löschung oder Sperrung von Daten) in Bezug auf personenbezogene Daten von Kyndryl geltend zu machen, informieren. Der Lieferant kann eine betroffene Person, die einen solchen Antrag stellt, auch direkt an Kyndryl verweisen. Der Lieferant wird keine Anträge von betroffenen Personen beantworten, außer wenn er gesetzlich dazu verpflichtet ist oder von Kyndryl schriftlich zur Beantwortung aufgefordert wird.

3.2 Wenn Kyndryl verpflichtet ist, Informationen in Bezug auf personenbezogene Daten von Kyndryl sonstigen Verantwortlichen oder Dritten (z. B. betroffenen Personen oder Regulierungsbehörden) bereitzustellen, wird der Lieferant Kyndryl unterstützen, indem er Informationen bereitstellt und andere angemessene Maßnahmen ergreift, wie von Kyndryl verlangt und nach einem Zeitplan, der es Kyndryl ermöglicht, rechtzeitig auf die sonstigen Verantwortlichen oder Dritten zuzugehen.

4. Unterauftragsverarbeiter

4.1 Der Lieferant verpflichtet sich, Kyndryl vor Aufnahme eines neuen Unterauftragsverarbeiters oder Erweiterung des Verarbeitungsumfangs durch einen bestehenden Unterauftragsverarbeiter schriftlich unter Angabe des Namens des Unterauftragsverarbeiters und der Beschreibung des neuen oder erweiterten Verarbeitungsumfangs zu benachrichtigen. Kyndryl kann gegen einen solchen neuen Unterauftragsverarbeiter oder erweiterten Umfang jederzeit aus angemessenen Gründen Einspruch erheben. In diesem Fall werden die Parteien zusammenarbeiten, um sich einvernehmlich mit dem Einspruch von Kyndryl zu befassen. Vorbehaltlich des Rechts von Kyndryl, jederzeit Einspruch zu erheben, kann der Lieferant den neuen Unterauftragsverarbeiter beauftragen oder den Verarbeitungsumfang des bestehenden Unterauftragsverarbeiters erweitern, falls Kyndryl innerhalb von 30 Tagen nach dem Datum der schriftlichen Benachrichtigung des Lieferanten keinen Einwand erhoben hat.

4.2 Der Lieferant verpflichtet sich, die in diesen Bedingungen festgelegten Verpflichtungen hinsichtlich Datenschutz, Datensicherheit und Zertifizierung an jeden genehmigten Unterauftragsverarbeiter weiterzugeben, bevor ein Unterauftragsverarbeiter Kyndryl Daten verarbeitet. Der Lieferant haftet gegenüber Kyndryl umfassend für die Erfüllung der Verpflichtungen der einzelnen Unterauftragsverarbeiter.

5. Grenzüberschreitende Datenverarbeitung

In Übereinstimmung mit nachstehender Verwendung gilt Folgendes:

Land mit angemessenem Schutz bezeichnet ein Land, das gemäß dem anwendbaren Datenschutzrecht oder den Entscheidungen von Regulierungsbehörden ein angemessenes Datenschutzniveau in Bezug auf die jeweilige Übermittlung bietet.

Datenimporteur bezeichnet einen Auftragsverarbeiter oder Unterauftragsverarbeiter, der nicht in einem Land mit angemessenem Schutz niedergelassen ist.

EU-Standardvertragsklauseln bezeichnet die EU-Standardvertragsklauseln (Beschluss der Kommission 2021/914) unter Anwendung der fakultativen Klauseln, mit Ausnahme von Option 1 von Klausel 9(a) und Option 2 von Klausel 17, die offiziell unter https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en veröffentlicht sind.

Serbische Standardvertragsklauseln bezeichnet die Serbischen Standardvertragsklauseln in der vom „Serbian Commissioner for Information of Public Importance and Personal Data Protection“ verabschiedeten Form, die unter https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx veröffentlicht sind.

Standardvertragsklauseln bezeichnet die Vertragsklauseln, die anwendbares Datenschutzrecht für die Übermittlung personenbezogener Daten an Auftragsverarbeiter fordert, die nicht in einem Land mit angemessenem Schutz niedergelassen sind.

Zusatzvereinbarung des Vereinigten Königreichs hinsichtlich der internationalen Datenübermittlung zu den Standardvertragsklauseln der EU-Kommission ("Zusatzvereinbarung des Vereinigten Königreichs") bezeichnet die Zusatzvereinbarung des Vereinigten Königreichs hinsichtlich der internationalen Datenübermittlung zu den Standardvertragsklauseln der EU-Kommission in der offiziell unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/ veröffentlichten Fassung.

5.1 Der Lieferant wird keine personenbezogenen Daten von Kyndryl ohne vorherige schriftliche Zustimmung von Kyndryl grenzüberschreitend übermitteln oder offenlegen (auch nicht per

Fernzugriff). Wenn Kyndryl eine solche Zustimmung bereitstellt, werden die Parteien zusammenarbeiten, um die Einhaltung von anwendbarem Datenschutzrecht sicherzustellen. Falls gemäß anwendbarem Datenschutzrecht Standardvertragsklauseln erforderlich sind, wird der Lieferant auf Anforderung von Kyndryl diese unverzüglich aufnehmen.

5.2 In Bezug auf EU-Standardvertragsklauseln gilt Folgendes:

(a) Wenn der Lieferant nicht in einem Land mit angemessenem Schutz niedergelassen ist, schließt der Lieferant als Datenimporteur mit Kyndryl EU-Standardvertragsklauseln und schriftliche Vereinbarungen mit allen genehmigten Unterauftragsverarbeitern in Übereinstimmung mit Klausel 9 der EU-Standardvertragsklauseln ab und stellt Kyndryl auf Anforderung Kopien dieser Vereinbarungen bereit.

(i) Modul 1 der EU-Standardvertragsklauseln kommt nicht zur Anwendung, sofern von den Parteien nicht abweichend schriftlich vereinbart.

(ii) Modul 2 der EU-Standardvertragsklauseln kommt zur Anwendung, wenn Kyndryl ein Verantwortlicher ist, und Modul 3 kommt zur Anwendung, wenn Kyndryl ein Auftragsverarbeiter ist. Wenn Modul 2 oder 3 Anwendung findet, vereinbaren die Parteien in Übereinstimmung mit Klausel 13 der EU-Standardvertragsklauseln, dass (1) die EU-Standardvertragsklauseln dem Recht des EU-Mitgliedstaats unterliegen, in dem die zuständige Aufsichtsbehörde ihren Sitz hat, und (2) alle Streitigkeiten, die sich aus den EU-Standardvertragsklauseln ergeben, an die Gerichte des EU-Mitgliedstaats verwiesen werden, in dem die zuständige Aufsichtsbehörde ihren Sitz hat. Wenn dieses Recht in (1) keine Rechte als Drittbegünstigte zulässt, unterliegen die EU-Standardvertragsklauseln dem Recht der Niederlande und alle Streitigkeiten, die sich aus den EU-Standardvertragsklauseln unter (2) ergeben, werden von einem Gericht in Amsterdam in den Niederlanden beigelegt.

(b) Wenn der Lieferant im Europäischen Wirtschaftsraum niedergelassen ist und Kyndryl ein Verantwortlicher ist, der nicht der Datenschutz-Grundverordnung 2016/679 unterliegt, dann kommt Modul 4 der EU-Standardvertragsklauseln zur Anwendung, und der Lieferant schließt als Datenexporteur mit Kyndryl EU-Standardvertragsklauseln ab. Wenn Modul 4 der EU-Standardvertragsklauseln zur Anwendung kommt, vereinbaren die Parteien, dass die EU-Standardvertragsklauseln dem Recht der Niederlande unterliegen und alle Streitigkeiten, die sich aus den EU-Standardvertragsklauseln ergeben, von einem Gericht in Amsterdam in den Niederlanden beigelegt werden.

(c) Falls sonstige Verantwortliche, wie z. B. Kunden oder verbundene Unternehmen, beantragen, den EU-Standardvertragsklauseln gemäß der 'Kopplungsklausel' in Klausel 7 als Partei beizutreten, stimmt der Lieferant hiermit einem solchen Antrag zu.

(d) Die technischen und organisatorischen Maßnahmen, die in Anhang II der EU-Standardvertragsklauseln ausgefüllt werden müssen, sind in diesen Bedingungen, im Auftragsdokument selbst und in der zugehörigen Rahmenvereinbarung zwischen den Parteien zu finden.

(e) Bei Widersprüchen zwischen den EU-Standardvertragsklauseln und diesen Bedingungen haben die EU-Standardvertragsklauseln Vorrang.

5.3 Zusatzvereinbarung(en), die das Vereinigte Königreich betrifft/betreffen:

a) Falls der Anbieter nicht in einem geeigneten Land ansässig ist: (i) schließt der Anbieter hiermit mit Kyndryl als Importeur einen oder mehrere britische Zusatzvereinbarungen ab, um die oben genannten EU-SCCs zu ergänzen (je nach den Umständen der Verarbeitungstätigkeiten); und (ii) schließt der Anbieter schriftliche Vereinbarungen mit jedem zugelassenen Unterverarbeiter ab und stellt Kyndryl auf Anfrage Kopien dieser Vereinbarungen zur Verfügung.

b) Wenn der Anbieter in einem geeigneten Land ansässig ist und Kyndryl ein für die Verarbeitung Verantwortlicher ist, der nicht der Allgemeinen Datenschutzverordnung des Vereinigten Königreichs (in der Fassung des European Union (Withdrawal) Act 2018) unterliegt, schließt der Anbieter hiermit als Exporteur mit Kyndryl ein oder mehrere Zusatzvereinbarungen für das Vereinigte Königreich ab, die den in Abschnitt 5.2(b) oben aufgeführten EU-SCCs beigefügt werden.

c) Wenn andere Verantwortliche, wie Kunden oder verbundene Unternehmen, beantragen, Vertragspartei des/der Zusatzvereinbarungen des Vereinigten Königreichs zu werden, erklärt sich der Anbieter hiermit mit einem solchen Antrag einverstanden.

d) Die Zusatzangaben (wie in Tabelle 3 aufgeführt) in dem/den Nachtrag(en) für das Vereinigte Königreich sind in den anwendbaren EU-SCCs, diesen Geschäftsbedingungen, dem Transaktionsdokument selbst und dem zugehörigen Rahmenvertrag zwischen den Parteien zu finden. Weder Kyndryl noch der Anbieter können den/die Zusatzvereinbarungen für das Vereinigte Königreich beenden, wenn sich die Zusatzvereinbarungen für das Vereinigte Königreich ändern.

e) Im Falle eines Widerspruchs zwischen den Zusatzvereinbarungen für das Vereinigte Königreich und den vorliegenden Bedingungen haben die Zusatzvereinbarungen für das Vereinigte Königreich Vorrang.

5.4 In Bezug auf die Serbischen Standardvertragsklauseln gilt Folgendes:

(a) Wenn der Lieferant nicht in einem Land mit angemessenem Schutz niedergelassen ist, (i) schließt der Lieferant im eigenen Namen als Auftragsverarbeiter mit Kyndryl Serbische Standardvertragsklauseln und (ii) schriftliche Vereinbarungen mit allen genehmigten Unterauftragsverarbeitern in Übereinstimmung mit Artikel 8 der Serbischen Standardvertragsklauseln ab und stellt Kyndryl auf Anforderung Kopien dieser Vereinbarungen bereit.

(b) Wenn der Lieferant in einem Land mit angemessenem Schutz niedergelassen ist, schließt der Lieferant mit Kyndryl im Namen aller Unterauftragsverarbeiter, die in einem Land ohne angemessenen Schutz ansässig sind, Serbische Standardvertragsklauseln ab. Sollte der Lieferant dies nicht für alle Unterauftragsverarbeiter tun können, stellt er Kyndryl die von diesem Unterauftragsverarbeiter unterzeichneten Serbischen Standardvertragsklauseln zur Gegenzeichnung durch Kyndryl bereit, bevor er dem Unterauftragsverarbeiter gestattet, personenbezogene Daten von Kyndryl zu verarbeiten.

(c) Die Serbischen Standardvertragsklauseln zwischen Kyndryl und dem Lieferanten dienen als Serbische Standardvertragsklauseln zwischen einem Verantwortlichen und Auftragsverarbeiter oder als schriftliche Back-to-Back-Vereinbarung zwischen dem 'Auftragsverarbeiter' und dem 'Unterauftragsverarbeiter', wie es die Faktenlage erfordert. Bei Widersprüchen zwischen den Serbischen Standardvertragsklauseln und diesen Bedingungen haben die Serbischen Standardvertragsklauseln Vorrang.

(d) Informationen, die zum Ausfüllen der Anhänge 1 bis 8 der Serbischen Standardvertragsklauseln notwendig sind und die Übermittlung personenbezogener Daten in ein Land ohne angemessenen Schutz betreffen, sind in diesen Bedingungen und in der Anlage zum Auftragsdokument oder im Auftragsdokument selbst zu finden.

6. Unterstützung und Verzeichnis

6.1 Unter Berücksichtigung der Art der Verarbeitung unterstützt der Lieferant Kyndryl mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Verpflichtungen in Verbindung mit Anträgen und Rechten Betroffener. Der Lieferant unterstützt Kyndryl darüber hinaus bei der Einhaltung von Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Meldung und

Weitergabe einer Sicherheitsverletzung und die Erstellung von Datenschutz-Folgenabschätzungen, einschließlich, sofern erforderlich, der vorherigen Konsultation mit der zuständigen Regulierungsbehörde, unter Berücksichtigung der dem Lieferanten zur Verfügung stehenden Informationen.

6.2 Der Lieferant verpflichtet sich, ein aktuelles Verzeichnis der Namen und Kontaktdaten der einzelnen Unterauftragsverarbeiter, einschließlich der Vertreter und Datenschutzbeauftragten der Unterauftragsverarbeiter, zu führen. Auf Anforderung stellt der Lieferant Kyndryl dieses Verzeichnis nach einem Zeitplan bereit, der es Kyndryl ermöglicht, rechtzeitig auf die Nachfrage eines Kunden oder Dritten zu reagieren.

Artikel IV, Technische und organisatorische Maßnahmen, Codesicherheit

Dieser Artikel gilt, wenn der Lieferant Zugriff auf Kyndryl Quellcode hat. Der Lieferant wird die Anforderungen dieses Artikels einhalten und dabei Kyndryl Quellcode vor Verlust, Vernichtung, Veränderung, versehentlicher oder nicht autorisierter Offenlegung, versehentlichem oder unbefugtem Zugriff und rechtswidriger Handhabung schützen. Die Anforderungen dieses Artikels erstrecken sich auf alle IT-Anwendungen, -Plattformen und -Infrastrukturen, die der Lieferant im Rahmen der Bereitstellung von Waren und Leistungen und der Handhabung von Kyndryl Technologie betreibt oder verwaltet, einschließlich aller Entwicklungs-, Test-, Hosting-, Support-, Betriebs- und Rechenzentrumsumgebungen.

1. Sicherheitsanforderungen

In Übereinstimmung mit nachstehender Verwendung gilt Folgendes:

Ausgeschlossenes Land bezeichnet ein Land, das (a) die US-Regierung gemäß Verfügung des Präsidenten zum Schutz der Lieferkette für Informations- und Kommunikationstechnologie sowie -services (Executive Order on Securing the Information and Communications Technology and Services Supply Chain) vom 15. Mai 2019 als ausländische Widersacher bezeichnet hat, (b) in Abschnitt 1654 des U.S. National Defense Authorization Act von 2019 aufgeführt ist oder (c) im Auftragsdokument als „ausgeschlossenes Land“ identifiziert wird.

1.1. Der Lieferant wird Kyndryl Quellcode nicht zugunsten von Dritten weitergeben oder treuhänderisch verwahren.

1.2. Der Lieferant wird verhindern, dass Kyndryl Quellcode auf Servern in einem ausgeschlossenen Land gespeichert wird. Der Lieferant untersagt jedem, einschließlich seiner Mitarbeiter, der in einem ausgeschlossenen Land ansässig ist oder ein ausgeschlossenes Land aus beliebigem Grund besucht (für die Dauer dieses Besuchs), den Zugriff auf Kyndryl Quellcode oder dessen Verwendung, unabhängig davon, wo sich dieser Kyndryl Quellcode weltweit befindet. Ferner verbietet der Lieferant Entwicklungs-, Test- oder sonstige Arbeiten in einem ausgeschlossenen Land, die entsprechenden Zugriff oder entsprechende Verwendung erfordern.

1.3. Der Lieferant wird Kyndryl Quellcode nicht in Rechtsordnungen platzieren oder weitergeben, in denen geltendes Recht oder die Rechtsauslegung die Offenlegung von Quellcode gegenüber Dritten erfordert. Falls es in einer Rechtsordnung, in der sich Kyndryl Quellcode befindet, zu einer Änderung geltenden Rechts oder der Rechtsauslegung kommt, aufgrund der der Lieferant den Quellcode gegenüber einem Dritten offenlegen muss, wird der Lieferant betreffenden Kyndryl Quellcode umgehend löschen oder aus dieser Rechtsordnung entfernen und keinen weiteren Kyndryl Quellcode in dieser Rechtsordnung platzieren, sofern dieses Recht oder diese Rechtsauslegung in Kraft bleibt.

1.4. Der Lieferant wird weder direkt noch indirekt eine Maßnahme ergreifen, z. B. eine Vereinbarung abschließen, die dazu führt, dass für den Lieferanten, Kyndryl oder einen Dritten eine Offenlegungsverpflichtung gemäß Abschnitt 1654 oder 1655 des U.S. National Defense Authorization Act von 2019 wirksam wird. Genauer gesagt, ist der Lieferant unter keinen Bedingungen berechtigt, Kyndryl Quellcode ohne die vorherige schriftliche Zustimmung von Kyndryl gegenüber Dritten offenzulegen, es sei denn, dies ist im Auftragsdokument oder in einer zugehörigen Rahmenvereinbarung zwischen den Parteien ausdrücklich zulässig.

1.5. Wenn Kyndryl den Lieferanten oder ein Dritter eine der Parteien über Folgendes benachrichtigt: Der Lieferant hat (a) zugelassen, dass Kyndryl Quellcode in ein ausgeschlossenes Land oder eine Rechtsordnung gemäß Abschnitt 1.3 oben gelangt, (b) Kyndryl Quellcode auf eine Art und Weise freigegeben, abgerufen oder verwendet, die nicht durch das Auftragsdokument oder eine zugehörige Rahmen- oder sonstige Vereinbarung zwischen den Parteien autorisiert ist, oder (c) gegen Abschnitt 1.4 oben verstoßen, gilt Folgendes, ohne die Rechte von Kyndryl zur rechtlichen Verfolgung dieser Nichteinhaltung oder zur Verfolgung unter dem Auftragsdokument oder einer zugehörigen Rahmen- oder sonstigen Vereinbarung zwischen den Parteien einzuschränken: (i) Falls eine solche Benachrichtigung an den Lieferanten gerichtet ist, gibt der Lieferant diese umgehend an Kyndryl weiter, und (ii) wird der Lieferant auf angemessene Weisung von Kyndryl die Angelegenheit nach dem Zeitplan

untersuchen und beilegen, den Kyndryl in angemessenem Rahmen festlegt (nach Absprache mit dem Lieferanten).

1.6. Sollte Kyndryl nach bestem Wissen der Ansicht sein, dass Änderungen an Richtlinien, Prozeduren, Kontrollmechanismen oder Verfahren des Lieferanten in Bezug auf den Zugriff auf Quellcode notwendig sind, um Risiken hinsichtlich Cybersicherheit, Diebstahl geistigen Eigentums oder vergleichbare oder zugehörige Risiken anzugehen (einschließlich des Risikos, dass Kyndryl ohne diese Änderungen möglicherweise nicht mehr in der Lage ist, an bestimmte Kunden oder in bestimmte Märkte zu verkaufen oder Sicherheits- oder Lieferkettenanforderungen anderweitig zu erfüllen), kann Kyndryl den Lieferanten kontaktieren, um die erforderlichen Maßnahmen zu besprechen, um diese Risiken, einschließlich Änderungen an diesen Richtlinien, Prozeduren, Kontrollmechanismen oder Verfahren zu adressieren. Auf Anforderung von Kyndryl verpflichtet sich der Lieferant zur Zusammenarbeit mit Kyndryl bei der Beurteilung, ob diese Änderungen notwendig sind, und bei der Implementierung geeigneter, gemeinsam vereinbarter Änderungen.

Artikel V, Sichere Entwicklung

Dieser Artikel gilt, wenn der Lieferant Kyndryl seinen Quellcode oder Quellcode anderer Anbieter oder On-Premises-Software zur Verfügung stellt oder wenn Waren oder Leistungen des Lieferanten einem Kyndryl Kunden als Bestandteil eines Kyndryl Produkts oder Service bereitgestellt werden.

1. Sicherheitsbereitschaft

Der Lieferant wird an den internen Prozessen von Kyndryl mitwirken, die die Sicherheitsbereitschaft von Kyndryl Produkten und Services bewerten, die wiederum von Waren des Lieferanten abhängen. Dies schließt die rechtzeitige und umfassende Reaktion auf Informationsanforderungen, z. B. über Dokumente, sonstige Aufzeichnungen, Befragungen relevanter Mitarbeiter des Lieferanten oder Ähnliches, ein.

2. Sichere Entwicklung

2.1 Dieser Abschnitt gilt nur, wenn der Lieferant Kyndryl On-Premises-Software zur Verfügung stellt.

2.2 Der Lieferant hat in Übereinstimmung mit branchenüblichen Best Practices Sicherheitsrichtlinien, -verfahren und -kontrollen in Bezug auf das Netzwerk, die Plattform, Systeme, Anwendungen, Geräte, die physische Infrastruktur, Störfallbehebung und Mitarbeiter implementiert, die erforderlich sind, um (a) die Entwicklungs-, Build-, Test- und Betriebssysteme und -umgebungen, die der Lieferant oder ein von ihm beauftragter Dritter für oder im Zusammenhang mit den Waren betreibt, verwaltet, verwendet oder auf die er sich anderweitig stützt, und (b) den gesamten Quellcode der Waren vor Verlust, unrechtmäßiger Handhabung und unbefugtem Zugriff, Offenlegung oder Änderung zu schützen und wird diese während der Laufzeit des Auftragsdokuments aufrechterhalten.

3. ISO 20243 Zertifizierung

3.1 Dieser Abschnitt 3 gilt nur, wenn Waren oder Leistungen des Lieferanten einem Kyndryl Kunden als Bestandteil eines Kyndryl Produkts oder Service bereitgestellt werden.

3.2 Der Lieferant verpflichtet sich, eine Zertifizierung der Einhaltung von ISO 20243, Informationstechnik – Open Trusted Technologie-Provider-Standard (O-TTPS) – Maßnahmen gegen korrumpierte und gefälschte Produkte, (entweder eine selbst-bewertete Zertifizierung oder eine Zertifizierung basierend auf der Bewertung eines angesehenen externen Prüfers) zu beschaffen. Alternativ gilt Folgendes: Auf schriftliche Anforderung des Lieferanten und nach schriftlicher Genehmigung durch Kyndryl wird der Lieferant eine Zertifizierung der Einhaltung eines im Wesentlichen vergleichbaren Branchenstandards mit Bezug auf sichere Entwicklungs- und Lieferkettenverfahren (entweder eine selbst-bewertete Zertifizierung oder eine Zertifizierung basierend auf der Bewertung eines angesehenen externen Prüfers, sofern von Kyndryl genehmigt) beschaffen.

3.3 Der Lieferant wird die Zertifizierung der Einhaltung von ISO 20243 oder eines im Wesentlichen vergleichbaren Branchenstandards (sofern schriftlich von Kyndryl genehmigt) innerhalb von 180 Tagen nach dem Wirksamkeitsdatum des Auftragsdokuments einholen und danach alle 12 Monate verlängern (wobei jede Verlängerung anhand der jeweils aktuellsten Version des jeweiligen Standards, d. h. ISO 20243 oder, sofern von Kyndryl schriftlich genehmigt, eines im Wesentlichen vergleichbaren Branchenstandards erfolgen muss, der sich auf sichere Entwicklungs- und Lieferkettenverfahren bezieht).

3.4 Der Lieferant wird Kyndryl auf Anforderung unverzüglich eine Kopie der Zertifizierungen bereitstellen, zu deren Einholung er gemäß den vorstehenden Abschnitten 2.1 und 2.2 verpflichtet ist.

4. Sicherheitslücken

In Übereinstimmung mit nachstehender Verwendung gilt Folgendes:

Fehlerkorrektur bezeichnet Fixes und Überarbeitungen, durch die Fehler oder Mängel, einschließlich Sicherheitslücken, in Waren behoben werden.

Maßnahmen zur Risikominderung bezeichnet alle bekannten Maßnahmen zur Verringerung oder Vermeidung der Risiken, die durch eine Sicherheitslücke entstehen.

Sicherheitslücke bezeichnet eine Schwachstelle im Design oder Code, in der Entwicklung oder Implementierung, bei Test, Betrieb, Unterstützung, Wartung oder Verwaltung einer Ware, die für einen Angriff durch Dritte, der unbefugte Zugriffe oder Nutzungen zur Folge haben könnte, wie z. B. (a) Zugriff auf ein System, Kontrolle oder Unterbrechung des Systembetriebs, (b) Zugriff auf Daten, Löschen, Ändern oder Extrahieren von Daten oder (c) Änderungen der Identität, Berechtigungen oder Genehmigungen von Benutzern oder Administratoren, genutzt werden kann. Eine Sicherheitslücke kann vorliegen, unabhängig davon, ob ihr eine CVE-ID (Common Vulnerabilities and Exposures), eine andere Einstufung (Score) oder eine offizielle Klassifizierung zugeordnet wurde.

4.1 Der Lieferant gewährleistet, dass er (a) branchenübliche Best Practices zur Aufdeckung von Sicherheitslücken anwenden wird, einschließlich durch fortlaufende statische und dynamische Überprüfung der Anwendungssicherheit anhand des Quellcodes, durch Überprüfung der Open-Source-Sicherheit und durch Überprüfung von Systemsicherheitslücken, und (b) die Anforderungen dieser Bedingungen einhalten wird, um Sicherheitslücken in Waren und allen IT-Anwendungen, -Plattformen und -Infrastrukturen, in denen und über die der Lieferant Leistungen und Waren erstellt und bereitstellt, zu verhindern, zu erkennen und zu beheben.

4.2 Wenn der Lieferant Kenntnis von einer Sicherheitslücke in einer Ware oder IT-Anwendung, -Plattform oder -Infrastruktur erlangt, wird er Kyndryl eine Fehlerkorrektur bereitstellen und Maßnahmen zur Risikominderung für alle Versionen und Releases der Waren durchführen, die auf die in den nachstehenden Tabellen definierten Schweregrade und Fristen abgestimmt sind.

Schweregrad*
Notfall-Sicherheitslücke bezeichnet eine Sicherheitslücke, die eine schwerwiegende und potenziell globale Bedrohung darstellt. Kyndryl benennt Notfall-Sicherheitslücken nach eigenem Ermessen, unabhängig vom CVSS-Basisscore.
Kritisch bezeichnet eine Sicherheitslücke mit einem CVSS-Basisscore von 9 bis 10.0
Hoch bezeichnet eine Sicherheitslücke mit einem CVSS-Basisscore von 7.0 bis 8.9
Mittel bezeichnet eine Sicherheitslücke mit einem CVSS-Basisscore von 4.0 bis 6.9
Gering bezeichnet eine Sicherheitslücke mit einem CVSS-Basisscore von 0.0 bis 3.9

Fristen				
Notfall	***Kritisch***	***Hoch***	***Mittel***	***Gering***
4 Tage oder weniger, nach Festlegung durch das Kyndryl Chief Information Security Office	30 Tage	30 Tage	90 Tage	Nach branchenüblichen Best Practices

* In allen Fällen, in denen einer Sicherheitslücke kein eindeutiger CVSS-Basisscore zugeordnet ist, wird der Lieferant einen Schweregrad anwenden, der für die Art und Umstände der Sicherheitslücke angemessen ist.

4.3 Falls der Lieferant Kyndryl für eine bereits veröffentlichte Sicherheitslücke noch keine Fehlerkorrektur bereitgestellt oder Maßnahmen zur Risikominderung durchgeführt hat, wird er alle technisch möglichen zusätzlichen Sicherheitsmaßnahmen implementieren, mit denen die Risiken der Sicherheitslücke verringert werden können.

4.4 Wenn Kyndryl mit der Reaktion des Lieferanten auf eine vorstehend beschriebene Sicherheitslücke in einer Ware oder Anwendung, Plattform oder Infrastruktur unzufrieden ist, wird sich der Lieferant,

vorbehaltlich aller sonstigen Rechte von Kyndryl, unverzüglich darum bemühen, dass Kyndryl seine Bedenken direkt mit einem Ressortleiter oder einer Führungskraft in einer vergleichbaren Position, die für die Bereitstellung der Fehlerkorrektur verantwortlich ist, erörtern kann.

4.5 Beispiele für Sicherheitslücken umfassen Code Dritter oder Open-Source-Code, dessen Servicezeitraum abgelaufen ist (End of Service, EOS), wenn für diese Codetypen keine Sicherheitsfixe mehr zur Verfügung gestellt werden.

Artikel VI, Zugriff auf Unternehmenssysteme

Dieser Artikel gilt, wenn Mitarbeiter des Lieferanten Zugriff auf Unternehmenssysteme haben.

1. Allgemeine Bedingungen

1.1 Kyndryl legt fest, ob Mitarbeiter des Lieferanten für den Zugriff auf Unternehmenssysteme autorisiert werden. Falls eine Autorisierung durch Kyndryl erfolgt, wird der Lieferant die zutreffenden Bedingungen einhalten und seine Mitarbeiter, die Zugriff haben, dazu verpflichten, die in diesem Artikel enthaltenen Vorgaben einzuhalten.

1.2 Kyndryl gibt die Mittel an, über die Mitarbeiter des Lieferanten auf Unternehmenssysteme zugreifen dürfen, einschließlich der Festlegung, ob der Zugriff dieser Mitarbeiter über von Kyndryl oder vom Lieferanten bereitgestellte Geräte erfolgt.

1.3 Mitarbeiter des Lieferanten dürfen nur für die Erbringung von Leistungen auf Unternehmenssysteme zugreifen und nur die Geräte verwenden, die Kyndryl für diesen Zugriff berechtigt. Mitarbeiter des Lieferanten dürfen die von Kyndryl berechtigten Geräte nicht verwenden, um Leistungen für eine andere natürliche oder juristische Person zu erbringen oder auf IT-Systeme, Netzwerke, Anwendungen, Websites, E-Mail-Tools, Tools für die Onlinezusammenarbeit oder ähnliche Lösungen des Lieferanten oder eines Dritten für die Leistungserbringung oder im Zusammenhang damit zuzugreifen.

1.4 Genauer gesagt, dürfen Mitarbeiter des Lieferanten die Geräte, die Kyndryl für den Zugriff auf Unternehmenssysteme berechtigt, nicht zu privaten Zwecken verwenden (z. B. dürfen Mitarbeiter des Lieferanten persönliche Dateien wie Musik, Videos, Bilder oder ähnliche Elemente nicht auf diesen Geräten speichern und das Internet nicht zu privaten Zwecken nutzen).

1.5 Mitarbeiter des Lieferanten verpflichten sich, Kyndryl Materialien, die über ein Unternehmenssystem zugänglich sind, ohne die vorherige schriftliche Genehmigung von Kyndryl nicht zu kopieren (und Kyndryl Materialien niemals auf ein portierbares Speichermedium, wie z. B. einen USB-Stick, eine externe Festplatte oder ähnliche Medien, zu kopieren).

1.6 Auf Anforderung wird der Lieferant die jeweiligen Unternehmenssysteme, auf die seine Mitarbeiter über einen von Kyndryl angegebenen Zeitraum zugreifen dürfen und bereits zugegriffen haben, nach Mitarbeiternamen bestätigen.

1.7 Der Lieferant wird Kyndryl innerhalb eines Zeitraums von vierundzwanzig (24) Stunden darüber benachrichtigen, wenn einer seiner Mitarbeiter mit Zugriff auf ein Unternehmenssystem nicht mehr (a) bei ihm beschäftigt ist oder (b) an Aktivitäten arbeitet, für die dieser Zugriff erforderlich ist. Der Lieferant wird mit Kyndryl zusammenarbeiten, um sicherzustellen, dass diesen ehemaligen oder aktuellen Mitarbeitern dieser Zugriff mit sofortiger Wirkung entzogen wird.

1.8 Der Lieferant wird Kyndryl umgehend alle tatsächlichen oder mutmaßlichen Sicherheitsvorfälle (z. B. den Verlust eines Geräts von Kyndryl oder vom Lieferanten oder den unbefugter Zugriff auf ein Gerät oder Daten, Materialien oder sonstige Informationen) melden und mit Kyndryl bei der Untersuchung dieser Vorfälle zusammenarbeiten.

1.9 Der Lieferant darf seinen Beauftragten, unabhängigen Auftragnehmern oder Mitarbeitern von Subunternehmern den Zugriff auf Unternehmenssysteme ohne vorherige schriftliche Zustimmung von Kyndryl nicht gestatten. Wenn Kyndryl diese Zustimmung erteilt, wird der Lieferant diese Personen und deren Arbeitgeber vertraglich dazu verpflichten, die in diesem Artikel enthaltenen Vorgaben einzuhalten, als handle es sich bei diesen Personen um Mitarbeiter des Lieferanten, und ist ferner gegenüber Kyndryl für alle Handlungen und Unterlassungen dieser Personen oder Arbeitgeber in Verbindung mit dem Zugriff auf Unternehmenssysteme verantwortlich.

2. Gerätesoftware

2.1 Der Lieferant wird seine Mitarbeiter dazu auffordern, sämtliche Gerätesoftware rechtzeitig zu installieren, die Kyndryl anfordert, um den sicheren Zugriff auf Unternehmenssysteme zu vereinfachen. Der Lieferant und seine Mitarbeiter verpflichten sich, die Operationen dieser Software oder der Sicherheitsfunktionen, die die Software aktiviert, nicht zu behindern.

2.2 Der Lieferant und seine Mitarbeiter werden die von Kyndryl festgelegten Regeln für die Gerätekonfiguration einhalten und anderweitig mit Kyndryl zusammenarbeiten, um sicherzustellen, dass die Software wie von Kyndryl beabsichtigt funktioniert. Beispielsweise wird der Lieferant nicht die Websiteblockierung oder automatisierte Patching-Funktionen der Software außer Kraft setzen.

2.3 Mitarbeiter des Lieferanten dürfen weder die Geräte, die sie für den Zugriff auf Unternehmenssysteme verwenden, noch ihre Benutzernamen, Kennwörter oder Ähnliches an Dritte weitergeben.

2.4 Wenn Kyndryl Mitarbeiter des Lieferanten für den Zugriff auf Unternehmenssysteme mit Geräten des Lieferanten autorisiert, wird der Lieferant auf diesen Geräten ein von Kyndryl genehmigtes Betriebssystem installieren und ausführen und innerhalb eines angemessenen Zeitraums nach Weisung von Kyndryl auf eine neue Version dieses Betriebssystems oder auf ein neues Betriebssystem aufrüsten.

3. Aufsicht und Mitwirkung

3.1 Kyndryl verfügt über uneingeschränkte Rechte zur Überwachung und Behebung potenzieller Angriffe von außen und sonstiger Cybersicherheitsbedrohungen auf beliebige Art und Weise, von beliebigen Standorten aus und unter Verwendung beliebiger Mittel, die Kyndryl für notwendig oder angemessen hält, ohne vorherige Benachrichtigung des Lieferanten oder eines Mitarbeiters des Lieferanten oder Dritter. Als Beispiel für diese Rechte kann Kyndryl jederzeit (a) Sicherheitstests auf Geräten durchführen, (b) Kommunikation (einschließlich E-Mails von beliebigen E-Mail-Konten), Datensätze, Dateien und sonstige Elemente, die auf einem Gerät gespeichert sind oder über ein Unternehmenssystem übertragen werden, überwachen, durch technische oder andere Mittel wiederherstellen und überprüfen und (c) ein vollständiges forensisches Image eines Geräts beschaffen. Falls Kyndryl die Mitwirkung des Lieferanten bei der Ausübung seiner Rechte benötigt, wird der Lieferant die Anforderungen von Kyndryl für eine solche Mitwirkung vollständig und rechtzeitig erfüllen (einschließlich Anforderungen in Bezug auf eine sichere Konfiguration eines Geräts, die Installation von Überwachungs- oder sonstiger Software auf einem Gerät, die Weitergabe von Verbindungsdetails auf Systemebene, die Beteiligung an Maßnahmen für die Störfallbehebung auf einem Gerät und die Bereitstellung von physischem Zugriff auf ein Gerät für Kyndryl, um ein vollständiges forensisches Image zu beschaffen, sowie vergleichbarer und zugehöriger Anforderungen).

3.2 Kyndryl kann den Zugriff auf Unternehmenssysteme durch einen oder alle Mitarbeiter des Lieferanten jederzeit und ohne vorherige Benachrichtigung des Lieferanten oder eines Mitarbeiters des Lieferanten oder Dritter entziehen, wenn Kyndryl der Ansicht ist, dass dies zum Schutz von Kyndryl erforderlich ist.

3.3 Die Rechte von Kyndryl werden durch eine im Auftragsdokument, in der zugehörigen Rahmenvereinbarung oder in einer sonstigen Vereinbarung zwischen den Parteien enthaltenen Bestimmung weder blockiert, abgeschwächt noch eingeschränkt. Dies gilt auch für Bestimmungen, die fordern, dass Daten, Materialien oder sonstige Informationen nur an einem bestimmten Standort oder an bestimmten Standorten gespeichert werden dürfen oder dass nur Personen von einem bestimmten Standort oder von bestimmten Standorten auf diese Daten, Materialien oder sonstigen Informationen zugreifen dürfen.

4. Kyndryl Geräte

4.1 Kyndryl behält das Eigentumsrecht an allen Kyndryl Geräten und der Lieferant übernimmt die Gefahrtragung in Bezug auf die Geräte, einschließlich aufgrund von Diebstahl, Vandalismus oder Fahrlässigkeit. Der Lieferant verpflichtet sich, ohne die vorherige schriftliche Zustimmung von Kyndryl keine Änderungen an Kyndryl Geräten vorzunehmen oder zu gestatten. Dabei handelt es sich um Änderungen an Geräten, einschließlich Änderungen an Software, Anwendungen, Sicherheitsplanung, Sicherheitskonfiguration oder am physischen, mechanischen oder elektrischen Design von Geräten.

4.2 Der Lieferant wird alle Kyndryl Geräte innerhalb von 5 Arbeitstagen, nachdem der Bedarf an diesen Geräten für die Leistungserbringung endet, zurückgeben und auf Anforderung von Kyndryl gleichzeitig alle Daten, Materialien und sonstigen Informationen auf diesen Geräten unter Einhaltung

branchenüblicher Best Practices für die dauerhafte Löschung dieser Daten, Materialien und sonstigen Informationen löschen, ohne Kopien davon aufzubewahren. Der Lieferant wird die Kyndryl Geräte verpacken und auf eigene Kosten an dem von Kyndryl benannten Standort in demselben Zustand zurückgeben, wie sie dem Lieferanten bereitgestellt wurden, angemessene Abnutzung ausgenommen. Sollte der Lieferant eine in diesem Abschnitt 4.2 enthaltene Verpflichtung nicht einhalten, stellt dies eine wesentliche Verletzung des Auftragsdokuments, der zugehörigen Rahmenvereinbarung und einer zugehörigen Vereinbarung zwischen den Parteien dar. Eine „zugehörige" Vereinbarung liegt vor, wenn der Zugriff auf ein Unternehmenssystem die Aufgaben oder sonstigen Aktivitäten des Lieferanten im Rahmen der jeweiligen Vereinbarung vereinfacht.

4.3 Kyndryl stellt Unterstützung für Kyndryl Geräte bereit (einschließlich Prüfung und vorbeugende sowie korrigierende Wartung der Geräte). Der Lieferant verpflichtet sich, Kyndryl unverzüglich über erforderliche Reparaturen zu informieren.

4.4 Für Softwareprogramme, die sich im Eigentum von Kyndryl befinden oder zu deren Lizenzierung Kyndryl berechtigt ist, erteilt Kyndryl dem Lieferanten das temporäre Recht zur Nutzung, Speicherung und Anfertigung einer ausreichenden Anzahl an Kopien, um die berechtigte Nutzung von Kyndryl Geräten zu unterstützen. Der Lieferant ist nicht berechtigt, Programme an Dritte zu übertragen, Kopien von Softwarelizenzinformationen zu erstellen oder ein Programm zu disassemblieren, zu dekompilieren, rückzuentwickeln oder anderweitig umzuwandeln, es sei denn, dass dies durch zwingende gesetzliche Regelung vorgesehen ist.

5. Aktualisierungen

5.1 Ungeachtet gegenteiliger Bedingungen im Auftragsdokument oder in der zugehörigen Rahmenvereinbarung zwischen den Parteien kann Kyndryl diesen Artikel durch schriftliche Benachrichtigung des Lieferanten und ohne die Zustimmung des Lieferanten einholen zu müssen, aktualisieren, ergänzen oder anderweitig ändern, um eine Anforderung gemäß geltendem Recht oder eine Verpflichtung gegenüber dem Kunden zu erfüllen und damit eine Entwicklung in Bezug auf Best Practices im Sicherheitsbereich abzubilden, oder wenn Kyndryl dies zum Schutz von Unternehmenssystemen oder von Kyndryl für notwendig erachtet.

Artikel VII, Mitarbeiterverstärkung

Dieser Artikel gilt, wenn Mitarbeiter des Lieferanten ihre Arbeitszeit vollständig für die Erbringung von Leistungen für Kyndryl nutzen, sie sämtliche Leistungen an Kyndryl Standorten, Kundenstandorten oder von Zuhause aus und nur unter Verwendung von Kyndryl Geräten für den Zugriff auf Unternehmenssysteme erbringen.

1. Zugriff auf Unternehmenssysteme; Kyndryl Umgebungen

1.1 Der Lieferant darf Leistungen nur durch Zugriff auf Unternehmenssysteme über Geräte, die von Kyndryl bereitgestellt werden, erbringen.

1.2 Der Lieferant verpflichtet sich zur Einhaltung der in Artikel VI (Zugriff auf Unternehmenssysteme) festgelegten Bedingungen für sämtlichen Zugriff auf Unternehmenssysteme.

1.3 Bei den von Kyndryl bereitgestellten Geräten handelt es sich um die einzigen Geräte, die der Lieferant und seine Mitarbeiter verwenden dürfen, um Leistungen zu erbringen. Die Geräte dürfen ferner vom Lieferanten und seinen Mitarbeitern nur für die Leistungserbringung verwendet werden. Genauer gesagt, dürfen der Lieferant oder seine Mitarbeiter keinesfalls andere Geräte für die Leistungserbringung verwenden oder Kyndryl Geräte für andere Kunden des Lieferanten oder andere Zwecke als die Leistungserbringung für Kyndryl verwenden.

1.4 Mitarbeiter des Lieferanten, die Kyndryl Geräte verwenden, können Kyndryl Materialien gemeinsam nutzen und diese Materialien auf den Kyndryl Geräten speichern, jedoch nur in dem begrenzten Umfang, in dem diese gemeinsame Nutzung und Speicherung notwendig ist, um die Leistungen erfolgreich zu erbringen.

1.5 Außer im Falle der Speicherung auf den Kyndryl Geräten, dürfen weder der Lieferant noch seine Mitarbeiter Kyndryl Materialien aus den Kyndryl Repositorys, Umgebungen, Tools oder Infrastrukturen entfernen, wo sie von Kyndryl gespeichert werden.

1.6 Genauer gesagt, sind der Lieferant und seine Mitarbeiter nicht berechtigt, Kyndryl Materialien ohne die vorherige schriftliche Zustimmung von Kyndryl an Repositorys, Umgebungen, Tool oder Infrastrukturen des Lieferanten oder an sonstige Systeme, Plattformen und Netzwerke des Lieferanten oder Ähnliches zu übertragen.

1.7 Artikel VIII (Technische und organisatorische Maßnahmen, allgemeine Sicherheit) gilt nicht für Leistungen des Lieferanten, wenn Mitarbeiter des Lieferanten ihre Arbeitszeit vollständig für die Erbringung von Leistungen für Kyndryl nutzen, sie sämtliche Leistungen an Kyndryl Standorten, Kundenstandorten oder von Zuhause aus und nur unter Verwendung von Kyndryl Geräten für den Zugriff auf Unternehmenssysteme erbringen. Ansonsten findet Artikel VIII für Leistungen des Lieferanten Anwendung.

Artikel VIII, Technische und organisatorische Maßnahmen, allgemeine Sicherheit

Dieser Artikel gilt, wenn der Lieferant Kyndryl Leistungen oder Waren bereitstellt, es sei denn, der Lieferant hat bei der Bereitstellung dieser Leistungen und Waren nur Zugriff auf geschäftsbezogene Kontaktinformationen von Kyndryl (d. h., der Lieferant verarbeitet keine sonstigen Kyndryl Daten und hat keinen Zugriff auf sonstige Kyndryl Materialien oder ein Unternehmenssystem), die einzigen Leistungen und Waren des Lieferanten bestehen in der Bereitstellung von On-Premises-Software oder der Lieferant stellt alle seine Leistungen und Waren gemäß Artikel VII, einschließlich Abschnitt 1.7, im Rahmen eines Modells für die Mitarbeiterverstärkung bereit.

Der Lieferant wird die Anforderungen dieses Artikels einhalten und dabei (a) Kyndryl Materialien vor Verlust, Vernichtung, Veränderung, versehentlicher oder nicht autorisierter Offenlegung sowie versehentlichem oder unbefugtem Zugriff, (b) Kyndryl Daten vor rechtswidriger Verarbeitung und (c) Kyndryl Technologie vor rechtswidriger Handhabung schützen. Die Anforderungen dieses Artikels erstrecken sich auf alle IT-Anwendungen, -Plattformen und -Infrastrukturen, die der Lieferant im Rahmen der Bereitstellung von Waren und Leistungen und der Handhabung von Kyndryl Technologie betreibt oder verwaltet, einschließlich aller Entwicklungs-, Test-, Hosting-, Support-, Betriebs- und Rechenzentrumsumgebungen.

1. Sicherheitsrichtlinien

1.1. Der Lieferant wird die IT-Sicherheitsrichtlinien und -verfahren, die ein integraler Bestandteil der Geschäftstätigkeit des Lieferanten und für alle Mitarbeiter des Lieferanten verbindlich sind und branchenüblichen Best Practices entsprechen, aufrechterhalten und befolgen.

1.2. Der Lieferant wird seine IT-Sicherheitsrichtlinien und -verfahren mindestens einmal jährlich überprüfen und ergänzen oder ändern, wenn er dies zum Schutz der Kyndryl Materialien für erforderlich hält.

1.3. Der Lieferant wird verbindliche Standardanforderungen in Bezug auf die Prüfung vorheriger Beschäftigungsverhältnisse aller neu eingestellten Beschäftigten festlegen und befolgen und diese Anforderungen auf alle Mitarbeiter und seine 100-prozentigen Tochtergesellschaften ausweiten. Zu diesen Anforderungen gehören die Überprüfung auf mögliche Vorstrafen, soweit gesetzlich zulässig, und eine Identitätsüberprüfung sowie zusätzliche Überprüfungen, die vom Lieferanten für notwendig erachtet werden. Der Lieferant wird diese Anforderungen regelmäßig erneut überprüfen, wenn er dies für notwendig erachtet.

1.4. Der Lieferant wird jährlich Schulungen zu Sicherheit und Datenschutz für seine Mitarbeiter durchführen und von seinen Mitarbeitern jedes Jahr verlangen, dass sie die Einhaltung der Grundsätze ethischen Verhaltens, der Vertraulichkeit und der Sicherheitsrichtlinien, die in den Verhaltensregeln oder vergleichbaren Dokumenten des Lieferanten festgelegt sind, nachweisen. Mitarbeiter mit Verwaltungszugriff auf Komponenten der Leistungen, Waren oder Kyndryl Materialien erhalten zusätzliche Schulungen zu Richtlinien und Prozessen, die speziell auf ihre Rolle und die Unterstützung der Leistungen, Waren und Kyndryl Materialien abgestimmt und zur Aufrechterhaltung der genannten Compliance-Nachweise und Zertifizierungen erforderlich sind.

1.5. Der Lieferant wird Sicherheits- und Datenschutzmaßnahmen entwickeln, um die Verfügbarkeit von Kyndryl Materialien zu schützen und aufrechtzuerhalten, insbesondere durch die Implementierung, Aufrechterhaltung und Einhaltung von Richtlinien und Verfahren, die Sicherheit und Datenschutz durch Technikgestaltung, sichere Entwicklung sowie sichere Arbeitsabläufe für alle Leistungen und Waren und für die Handhabung von Kyndryl Technologie verlangen.

2. Sicherheitsvorfälle

2.1. Der Lieferant wird dokumentierte Richtlinien zur Behebung von Sicherheitsvorfällen gemäß branchenüblichen Best Practices für den Umgang mit IT-Sicherheitsvorfällen etablieren und befolgen.

2.2. Der Lieferant wird unbefugten Zugriff und unbefugte Verwendung von Kyndryl Materialien untersuchen und einen entsprechenden Interventionsplan definieren und umsetzen.

2.3. Der Lieferant wird Kyndryl umgehend (jedoch spätestens innerhalb von 48 Stunden) benachrichtigen, wenn er Kenntnis über eine Sicherheitsverletzung erlangt. Diese Benachrichtigung erfolgt über das Kyndryl Global Procurement-Support-Portal unter https://www.kyndryl.com/procurement/procSupport. Der Lieferant wird Kyndryl auf Anforderung in angemessenem Umfang Informationen über eine solche Sicherheitsverletzung und den Status seiner Abhilfe- und Wiederherstellungsmaßnahmen bereitstellen. In angemessenem Rahmen geforderte

Informationen können beispielsweise Protokolle enthalten, die berechtigten, administrativen und sonstigen Zugriff auf Geräte, Systeme oder Anwendungen, forensische Abbildungen von Geräten, Systemen oder Anwendungen und andere vergleichbare Elemente nachweisen, sofern dies für die Sicherheitsverletzung oder die Abhilfe- und Wiederherstellungsmaßnahmen des Lieferanten relevant ist.

2.4. Der Lieferant wird Kyndryl angemessene Unterstützung bereitstellen, um rechtliche Verpflichtungen (einschließlich der Meldepflicht an Regulierungsbehörden oder betroffene Personen) von Kyndryl, Kyndryl Konzerngesellschaften und Kunden (sowie deren Kunden und verbundenen Unternehmen) in Zusammenhang mit einer Sicherheitsverletzung zu erfüllen.

2.5. Der Lieferant wird Dritte nur mit schriftlicher Genehmigung von Kyndryl oder im Falle einer gesetzlichen Meldepflicht darüber informieren, dass eine Sicherheitsverletzung direkt oder indirekt mit Kyndryl oder Kyndryl Materialien in Zusammenhang steht. Der Lieferant wird Kyndryl schriftlich davon in Kenntnis setzen, bevor er eine gesetzlich vorgeschriebene Mitteilung an Dritte weitergibt, aus der die Identität von Kyndryl direkt oder indirekt hervorgeht.

2.6. Im Falle einer Sicherheitsverletzung, die sich aus dem Verstoß gegen eine Verpflichtung im Rahmen dieser Bedingungen durch den Lieferanten ergibt, gilt Folgendes:

(a) Der Lieferant wird alle ihm entstehenden und Kyndryl tatsächlich entstandenen Kosten übernehmen, die durch die Meldung der Sicherheitsverletzung an zuständige Regulierungsbehörden, sonstige staatliche Stellen und etwaige relevante Branchen-Selbstregulierungsstellen, die Medien (sofern nach geltendem Recht erforderlich), betroffene Personen, Kunden und sonstige Dritte, verursacht werden,

(b) Auf Anforderung von Kyndryl wird der Lieferant auf eigene Kosten ein Call-Center einrichten, um Fragen von betroffenen Personen zu der Sicherheitsverletzung und deren Folgen zu beantworten, und für ein Jahr nach dem Datum, an dem diese betroffenen Personen über die Sicherheitsverletzung informiert wurden, oder gemäß den Anforderungen durch anwendbares Datenschutzrecht aufrechterhalten, je nachdem, welcher Zeitraum umfassenderen Schutz bietet. Kyndryl und der Lieferant werden die Scripts und sonstigen Materialien, die von den Mitarbeitern des Call-Centers bei der Beantwortung der Anfragen verwendet werden, gemeinsam erstellen. Nach schriftlicher Mitteilung an den Lieferanten kann Kyndryl alternativ ein eigenes Call-Center einrichten und aufrechterhalten, statt dies vom Lieferanten zu verlangen. In diesem Fall wird der Lieferant Kyndryl die tatsächlichen Kosten erstatten, die Kyndryl bei Einrichtung und Betrieb eines solchen Call-Centers entstehen.

(c) Der Lieferant wird Kyndryl die tatsächlichen Kosten der Bereitstellung von Kontoüberwachungsservices und Services zur Wiederherstellung der Bonitätsbewertung für ein Jahr nach dem Datum, an dem die Personen, die von der Sicherheitsverletzung betroffen waren und sich für die Services registriert hatten, über diese informiert wurden, oder gemäß den Anforderungen durch anwendbares Datenschutzrecht zurückerstatten, je nachdem, welcher Zeitraum umfassenderen Schutz bietet.

3. Physische Sicherheit und Zutrittskontrolle (gemäß nachstehender Verwendung bezeichnet „Einrichtung“ einen physischen Standort, an dem der Lieferant Kyndryl Materialien hostet, verarbeitet oder anderweitig darauf zugreift)

3.1. Der Lieferant wird geeignete physische Zutrittskontrollen, wie Schranken, durch Kartenleser kontrollierte Zutrittspunkte, Überwachungskameras und mit Personen besetzte Empfangsbereiche, einrichten, um die Einrichtungen vor unbefugtem Zutritt zu schützen.

3.2. Der Zugang zu den Einrichtungen und Kontrollbereichen innerhalb der Einrichtungen ist genehmigungspflichtig, einschließlich temporären Zugangs, und wird je nach ausgeübter Tätigkeit und geschäftlicher Notwendigkeit beschränkt. Wenn eine Person temporären Zugang erhält, wird ein autorisierter Mitarbeiter des Lieferanten den Besucher während seines Aufenthalts in der Einrichtung und den Kontrollbereichen begleiten.

3.3. Der Lieferant wird physische Zutritts- und Zugriffskontrollen, einschließlich mehrstufiger Zutrittskontrollen implementieren, die mit branchenüblichen Best Practices konform sind, um den Zugang zu Kontrollbereichen in den Einrichtungen angemessen zu beschränken, alle Zutrittsversuche protokollieren und diese Protokolle mindestens ein Jahr lang aufbewahren.

3.4. Der Lieferant wird (a) bei Ausscheiden oder Wechsel eines autorisierten Mitarbeiters oder (b) wenn der autorisierte Mitarbeiter keine geschäftliche Notwendigkeit mehr hat, den Zutritt zu den Einrichtungen und Kontrollbereichen in den Einrichtungen entziehen. Dabei befolgt der Lieferant die formalen dokumentierten Verfahren, die beim Ausscheiden oder Wechsel von Mitarbeitern einzuhalten sind, wie beispielsweise das unverzügliche Entfernen aus Zutrittskontrolllisten und die Rückgabe von Ausweisen und vieles mehr.

3.5. Der Lieferant wird Vorkehrungen treffen, um die gesamte physische Infrastruktur, die zur Unterstützung der Leistungen und Waren sowie zur Handhabung von Kyndryl Technologie eingesetzt wird, vor natürlichen als auch vor von Menschen verursachten Umweltgefahren zu schützen, wie beispielsweise extrem hohe Umgebungstemperatur, Feuer, Hochwasser, Feuchtigkeit, Diebstahl und Vandalismus.

4. Zugangs-, Zugriffs-, Weitergabe- und Trennungskontrolle

4.1. Der Lieferant wird die dokumentierte Sicherheitsarchitektur der von ihm verwalteten Netzwerke bei der Erbringung der Leistungen, der Bereitstellung der Waren und der Handhabung von Kyndryl Technologie aufrechterhalten. Dabei werden die Netzwerkarchitektur gesondert überprüft und Maßnahmen angewendet, die nicht autorisierte Netzwerkverbindungen zu Systemen, Anwendungen und Netzwerkgeräten verhindern sollen, um die Einhaltung der Standards für sichere Segmentierung, Isolation und tiefengestaffelte Verteidigung (In-depth Defense) sicherzustellen. Der Lieferant darf beim Hosting und Betrieb von Hosted Services keine Wireless-Technologie einsetzen; ansonsten ist bei der Bereitstellung der Leistungen und Waren und der Handhabung von Kyndryl Technologie der Einsatz von Wireless-Networking-Technologie erlaubt, der Lieferant muss allerdings Daten bei der Übertragung über drahtlose Netze verschlüsseln und sichere Authentifizierung für diese drahtlosen Netze verlangen.

4.2. Der Lieferant wird Maßnahmen ergreifen, die dazu ausgelegt sind, Kyndryl Materialien logisch zu trennen und zu verhindern, dass sie für Unbefugte verfügbar oder zugänglich sind. Des Weiteren wird der Lieferant Produktions-, Nicht-Produktions- und andere Umgebungen in angemessener Weise isolieren und, wenn Kyndryl Materialien bereits in einer Nicht-Produktionsumgebung vorhanden sind oder übertragen werden (z. B. zum Reproduzieren eines Fehlers), sicherstellen, dass die Sicherheits- und Datenschutzvorkehrungen in der Nicht-Produktionsumgebung denjenigen in der Produktionsumgebung entsprechen.

4.3. Der Lieferant wird Kyndryl Materialien bei der Übertragung und im Ruhezustand verschlüsseln (es sei denn, der Lieferant kann Kyndryl überzeugend nachweisen, dass die Verschlüsselung von Kyndryl Materialien im Ruhezustand technisch nicht realisierbar ist). Der Lieferant wird außerdem alle physischen Medien, soweit vorhanden, z. B. Medien, auf denen sich Sicherungsdateien befinden, verschlüsseln. Ferner müssen dokumentierte Verfahren für die sichere Erstellung, Ausgabe, Weitergabe, Speicherung, Rotation, den Widerruf sowie die Wiederherstellung, Sicherung, Löschung, den Zugriff auf und die Verwendung von Schlüsseln, die zur Datenverschlüsselung verwendet werden, etabliert werden. Dabei wird der Lieferant sicherstellen, dass die für diese Verschlüsselung angewendeten spezifischen Verschlüsselungsverfahren mit branchenüblichen Best Practices (wie z. B. NIST SP 800-131a) konform sind.

4.4. Wenn der Lieferant Zugriff auf Kyndryl Materialien benötigt, wird dieser auf die erforderliche Mindestberechtigungsstufe beschränkt, die für die Bereitstellung und Unterstützung der Leistungen und Waren erforderlich ist. Dieser Zugriff sowie der Verwaltungszugriff auf die zugrunde liegenden Komponenten (privilegierter Zugriff) muss individuell und rollenbasiert sein und regelmäßigen Prüfungen durch autorisierte Mitarbeiter des Lieferanten gemäß den Richtlinien für die Aufgabentrennung unterliegen. Der Lieferant wird Maßnahmen zur Aufdeckung und Löschung redundanter und inaktiver Konten ergreifen. Ferner wird der Lieferant Konten mit privilegiertem Zugriff innerhalb von vierundzwanzig (24) Stunden nach Ausscheiden des Kontoeigners oder auf Anforderung von Kyndryl oder autorisierten Mitarbeitern, wie beispielsweise durch den Vorgesetzten des Kontoeigners, löschen.

4.5. Im Einklang mit branchenüblichen Best Practices wird der Lieferant technische Maßnahmen umsetzen, die das Timeout inaktiver Sitzungen, die Sperrung von Konten nach mehreren aufeinanderfolgenden, fehlgeschlagenen Anmeldeversuchen und die Authentifizierung über sichere Kennwörter oder Kennphrasen erzwingen, sowie Maßnahmen, die eine sichere Übertragung und Speicherung dieser

Kennwörter und Kennphrasen verlangen. Zusätzlich wird der Lieferant Mehrfaktorauthentifizierung für alle nicht konsolenbasierten privilegierten Zugriffe auf Kyndryl Materialien anwenden.

4.6. Der Lieferant wird die Verwendung der privilegierten Zugriffe überwachen sowie Sicherheitsinformations- und Ereignismanagement-Maßnahmen ergreifen, um (a) unbefugte Zugriffe und Aktivitäten aufzudecken, (b) rechtzeitiges und angemessenes Reagieren auf derartige Zugriffe und Aktivitäten zu ermöglichen und (c) sowohl eigene Audits als auch Audits durch Kyndryl (gemäß den Prüfungsrechten in diesen Bedingungen und den Auditrechten im Auftragsdokument, in der zugehörigen Rahmenvereinbarung oder in sonstigen zugehörigen Vereinbarungen zwischen den Parteien) und Dritte auf Einhaltung der dokumentierten Richtlinie des Lieferanten zu ermöglichen.

4.7. Der Lieferant wird Protokolle aufbewahren, in denen gemäß branchenüblichen Best Practices alle Verwaltungs-, Benutzer- oder sonstigen Zugriffe oder Aktivitäten in Zusammenhang mit Systemen für die Bereitstellung von Leistungen und Waren und die Handhabung von Kyndryl Technologie aufgezeichnet werden (und wird diese Protokolle Kyndryl auf Anforderung zur Verfügung stellen). Der Lieferant wird Maßnahmen ergreifen, mit denen diese Protokolle vor unbefugtem Zugriff, unbefugter Änderung und zufälliger oder absichtlicher Zerstörung geschützt werden.

4.8. Der Lieferant wird Schutzmaßnahmen für Systeme in seinem Eigentum oder in seiner Verwaltung, einschließlich Endbenutzersystemen, und die er für die Bereitstellung von Leistungen oder Waren oder die Handhabung von Kyndryl Technologie verwendet, etablieren. Dazu gehören unter anderem Endpunktfirewalls, vollständige Plattenverschlüsselung, signaturbasierte und nicht signaturbasierte Endpoint-Detection-and-Response-Technologien für die Reaktion auf Malware-Bedrohungen und fortgeschrittene, andauernde Bedrohungen (Advanced Persistent Threats), zeitbasierte Bildschirmsperren und Endpunktmanagementlösungen, die Sicherheitskonfigurations- und Patching-Anforderungen durchsetzen. Ferner wird der Lieferant technische und betriebliche Kontrollmechanismen implementieren, die sicherstellen, dass nur bekannte und vertrauenswürdige Endbenutzersysteme für die Nutzung der Netze des Lieferanten zugelassen werden.

4.9. Im Einklang mit branchenüblichen Best Practices wird der Lieferant Schutzmaßnahmen für Rechenzentrumsumgebungen etablieren, in denen Kyndryl Materialien vorhanden sind oder verarbeitet werden, darunter die Erkennung und Verhinderung von unerlaubten Zugriffen (Intrusion Detection and Prevention) sowie Gegenmaßnahmen bei Denial-of-Service-Attacken und Maßnahmen zur Risikominderung.

5. Service- und Systemintegrität und Verfügbarkeitskontrolle

5.1. Der Lieferant wird (a) mindestens einmal jährlich Sicherheits- und Datenschutzrisikoabschätzungen durchführen, (b) vor der Freigabe für die Produktion und danach jährlich im Zusammenhang mit Leistungen und Waren sowie jährlich im Zusammenhang mit der Handhabung von Kyndryl Technologie Sicherheitstests und Schwachstellenanalysen, wie z. B. automatisierte Scans für System- und Anwendungssicherheit sowie präventives Hacken, durchführen, (c) einen qualifizierten unabhängigen Dritten damit beauftragen, mindestens einmal jährlich Penetrationstests in Übereinstimmung mit branchenüblichen Best Practices durchzuführen, wobei diese Tests sowohl automatisierte als auch manuelle Tests umfassen, (d) die automatisierte Verwaltung und Routineprüfung auf Einhaltung der Sicherheitskonfigurationsanforderungen für jede Komponente der Leistungen und Waren sowie im Zusammenhang mit der Handhabung von Kyndryl Technologie durchführen und (e) aufgedeckte Schwachstellen oder nicht eingehaltene Sicherheitskonfigurationsanforderungen abhängig von dem damit verbundenen Risiko, der Exploit-Anfälligkeit und der Auswirkung beheben. Der Lieferant wird angemessene Schritte unternehmen, um eine Unterbrechung von Leistungen bei der Ausführung der Tests, Prüfungen, Scans und Abhilfemaßnahmen zu vermeiden. Auf Anforderung wird der Lieferant Kyndryl einen schriftlichen Bericht der jüngsten Penetrationstestaktivitäten bereitstellen, der mindestens den Namen der Angebote und die Anzahl der Systeme oder Anwendungen, die in die Tests einbezogen wurden, die Testtermine, die bei den Tests angewendete Methodik und eine allgemeine Zusammenfassung der Ergebnisse enthält.

5.2. Der Lieferant wird Richtlinien und Verfahren anwenden, die für das Risikomanagement in Zusammenhang mit der Durchführung von Änderungen an den Leistungen oder Waren oder an der Handhabung von Kyndryl Technologie ausgelegt sind. Vor der Implementierung von Änderungen,

einschließlich an betroffenen Systemen, Netzen und zugrunde liegenden Komponenten, wird der Lieferant in einer registrierten Änderungsanforderung Folgendes dokumentieren: (a) eine Beschreibung sowie den Grund der Änderungen, (b) Einzelheiten der Implementierung und den Terminplan, (c) eine Risikoerklärung hinsichtlich der Auswirkung auf die Leistungen und Waren, Kunden der Leistungen oder Kyndryl Materialien, (d) das erwartete Ergebnis, (e) einen Rollback-Plan und (f) die Genehmigung durch autorisierte Mitarbeiter des Lieferanten.

5.3. Der Lieferant wird ein Inventar aller IT-Assets betriebsbereit halten, die er bei Erbringung der Leistungen, Bereitstellung der Waren und Handhabung der Kyndryl Technologie einsetzt. Der Zustand (einschließlich der Kapazität) und die Verfügbarkeit dieser IT-Assets, Leistungen, Waren und Kyndryl Technologie sowie der zugrunde liegenden Komponenten dieser Assets, Leistungen, Waren und Kyndryl Technologie werden vom Lieferanten fortlaufend überwacht und gesteuert.

5.4. Der Lieferant wird alle Systeme, die er für die Entwicklung oder Bereitstellung von Leistungen und Waren und die Handhabung von Kyndryl Technologie einsetzt, auf der Basis vordefinierter Systemsicherheitsimages oder grundlegender Sicherheitsregeln erstellen, die branchenüblichen Best Practices entsprechen, wie z. B. den Benchmarks des Center for Internet Security (CIS).

5.5. Ohne die Pflichten des Lieferanten oder die Rechte von Kyndryl aus dem Auftragsdokument oder der zugehörigen Rahmenvereinbarung zwischen den Parteien in Bezug auf unterbrechungsfreie Geschäftsabläufe (Business-Continuity) einzuschränken, wird der Lieferant jede Leistung und Ware sowie jedes IT-System, das für die Handhabung von Kyndryl Technologie verwendet wird, gemäß den dokumentierten Risikomanagementrichtlinien separat in Bezug auf Business- und IT-Continuity- sowie Disaster-Recovery-Anforderungen hin beurteilen. Der Lieferant wird sicherstellen, dass für jede Leistung und Ware sowie für jedes IT-System, soweit dies durch die Risikobeurteilung gerechtfertigt ist, separate Business- und IT-Continuity- sowie Disaster-Recovery-Pläne in Übereinstimmung mit branchenüblichen Best Practices definiert, dokumentiert, gepflegt und jährlich überprüft werden. Zudem muss sichergestellt werden, dass diese Pläne für die Einhaltung der in Abschnitt 5.6 unten angegebenen spezifischen Wiederherstellungszeiten ausgelegt sind.

5.6. Die spezifischen Recovery Point Objectives („**RPO**“) und Recovery Time Objectives („**RTO**“) in Bezug auf jeden Hosted Service lauten wie folgt: ein RPO von 24 Stunden und ein RTO von 24 Stunden. Unabhängig davon wird der Lieferant jedes kürzere RPO oder RTO, das Kyndryl einem Kunden zugesichert hat, unmittelbar nach der schriftlichen Mitteilung von Kyndryl über das kürzere RPO oder RTO einhalten (eine E-Mail stellt eine schriftliche Mitteilung dar). Da dies alle anderen vom Lieferanten für Kyndryl erbrachten Leistungen betrifft, wird der Lieferant sicherstellen, dass seine Business-Continuity- und Disaster-Recovery-Pläne für die Einhaltung dieser RPO- und RTO-Werte ausgelegt sind und ihm weiterhin die Einhaltung aller seiner Verpflichtungen gegenüber Kyndryl im Rahmen des Auftragsdokuments und der zugehörigen Rahmenvereinbarung zwischen den Parteien sowie diesen Bedingungen ermöglichen, einschließlich seiner Verpflichtungen in Bezug auf die rechtzeitige Bereitstellung von Testkapazitäten, Unterstützung und Wartung.

5.7. Der Lieferant wird Maßnahmen ergreifen, die dazu ausgelegt sind, Security Advisory Patches für die Leistungen und Waren und die zugehörigen Systeme, Netzwerke, Anwendungen und zugrunde liegenden Komponenten im Rahmen dieser Leistungen und Waren sowie die Systeme, Netzwerke, Anwendungen und zugrunde liegenden Komponenten, die zur Handhabung von Kyndryl Technologie verwendet werden, zu beurteilen, zu testen und einzuspielen. Wenn sich herausstellt, dass ein Security Advisory Patch anwendbar und geeignet ist, wird der Lieferant den Patch gemäß den dokumentierten Richtlinien zur Bewertung der Dringlichkeit und Risiken einspielen. Das Einspielen von Security Advisory Patches unterliegt der Change-Management-Richtlinie des Lieferanten.

5.8. Sollte Kyndryl einen angemessenen Grund zur Annahme haben, dass Hardware oder Software, die der Lieferant Kyndryl bereitstellt, intrusive Elemente, wie z. B. Spyware, Malware oder schädlichen Programmcode, enthält, wird der Lieferant rechtzeitig mit Kyndryl zusammenarbeiten, um die Bedenken von Kyndryl zu überprüfen und auszuräumen.

6. Serviceerbringung

6.1 Der Lieferant unterstützt branchenübliche Verfahren für die föderierte Authentifizierung von Kyndryl Benutzerkonten oder Kundenkonten, indem Kyndryl Benutzerkonten oder Kundenkonten (z. B. über zentral von Kyndryl verwaltetes Single Sign-on mit

Mehrfaktorauthentifizierung unter Verwendung von OpenID Connect oder Security Assertion Markup Language) in Übereinstimmung mit branchenüblichen Best Practices authentifiziert werden.

7. **Subunternehmer.** Ohne die Pflichten des Lieferanten oder die Rechte von Kyndryl aus dem Auftragsdokument oder der zugehörigen Rahmenvereinbarung zwischen den Parteien in Bezug auf die Bindung von Subunternehmern einzuschränken, wird der Lieferant sicherstellen, dass jeder Subunternehmer, der Arbeiten für den Lieferanten ausführt, Corporate-Governance-Kontrollen eingerichtet hat, um die Anforderungen und Verpflichtungen des Lieferanten im Rahmen dieser Bedingungen einzuhalten.
8. **Physische Medien**. Der Lieferant wird sämtliche Daten auf physischen Medien, die zur Wiederverwendung vorgesehen sind, vor einer erneuten Verwendung der Medien im Einklang mit branchenüblichen Best Practices für Medienbereinigung sicher löschen und physische Medien, die nicht zur Wiederverwendung vorgesehen sind, vernichten.

Artikel IX, Zertifizierungen und Berichte für Hosted Services

Dieser Artikel gilt, wenn der Lieferant Kyndryl einen Hosted Service bereitstellt.

1.1 Der Lieferant wird alle nachstehend aufgeführten Zertifizierungen oder Berichte innerhalb der angegebenen Fristen einholen:

Zertifizierungen/Berichte	**Frist**
Im Hinblick auf die Bereitstellung von Hosted Services durch den Lieferanten: Zertifizierung der Einhaltung von ISO 27001 (Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme), wobei diese Zertifizierung auf der Beurteilung eines angesehenen externen Prüfers basiert. **Oder** SOC 2 Typ 2: Ein Bericht eines angesehenen externen Prüfers, in dem der Prüfer nachweist, dass er die Systeme, Kontrollmechanismen und Betriebsabläufe gemäß SOC 2 Typ 2 (insbesondere in Bezug auf Sicherheit, Vertraulichkeit und Verfügbarkeit) geprüft hat.	Der Lieferant wird die ISO 27001-Zertifizierung innerhalb von 120 Tagen nach dem Wirksamkeitsdatum des Auftragsdokuments* oder dem Annahmedatum** einholen und danach alle 12 Monate basierend auf der Beurteilung eines angesehenen externen Prüfers verlängern (wobei jede Verlängerung anhand der jeweils aktuellsten Version des Standards erfolgen muss). Der Lieferant wird den SOC 2 Typ 2-Bericht innerhalb von 240 Tagen nach dem Wirksamkeitsdatum des Auftragsdokuments* oder dem Annahmedatum** einholen und danach alle 12 Monate von einem angesehenen externen Prüfer einen neuen Bericht einholen, in dem der Prüfer nachweist, dass er die Systeme, Kontrollmechanismen und Betriebsabläufe gemäß SOC 2 Typ 2 (insbesondere in Bezug auf Sicherheit, Vertraulichkeit und Verfügbarkeit) geprüft hat. * Wenn der Lieferant einen Hosted Service ab diesem Wirksamkeitsdatum bereitstellt ** Das Datum, an dem der Lieferant die Verpflichtung zur Bereitstellung des Hosted Service annimmt

1.2 Sofern vom Lieferanten schriftlich angefordert und von Kyndryl schriftlich genehmigt, kann der Lieferant im Wesentlichen gleichwertige Zertifizierungen oder Berichte wie die vorstehend genannten einholen, wobei die Parteien vereinbaren, dass die in der vorstehenden Tabelle angegebenen Fristen in Bezug auf die im Wesentlichen gleichwertigen Zertifizierungen oder Berichte unverändert gelten.

1.3 Der Lieferant wird (a) Kyndryl auf Anforderung unverzüglich eine Kopie jeder Zertifizierung und jedes Berichts bereitstellen, zu deren Einholung er verpflichtet ist, und (b) unverzüglich alle Schwachstellen in der internen Kontrolle, die bei den SOC 2-Prüfungen oder im Wesentlichen gleichwertigen Prüfungen (falls von Kyndryl genehmigt) festgestellt wurden, beheben.

Artikel X, Mitwirkung, Überprüfung und Fehlerbehebung

Dieser Artikel gilt, wenn der Lieferant Kyndryl Leistungen oder Waren bereitstellt.

1. Mitwirkung des Lieferanten

1.1. Falls Kyndryl Grund zur Annahme hat, dass Leistungen oder Waren möglicherweise zu Problemen mit der Cybersicherheit beigetragen haben, beitragen oder beitragen werden, wird der Lieferant an Kyndryl Anfragen in Bezug auf diese Probleme in angemessenem Umfang mitwirken. Dies schließt die rechtzeitige und umfassende Reaktion auf Informationsanforderungen, z. B. über Dokumente, sonstige Aufzeichnungen, Befragungen relevanter Mitarbeiter des Lieferanten oder Ähnliches, ein.

1.2. Die Parteien werden (a) sich auf Anforderung gegenseitig weitere Informationen bereitstellen, (b) weitere Dokumente unterzeichnen und sich gegenseitig bereitstellen und (c) weitere Maßnahmen und Aktionen durchführen, die die jeweils andere Partei in angemessenem Umfang anfordert, um die Absicht dieser Bedingungen und der in diesen Bedingungen genannten Dokumente umzusetzen. Beispiel: Auf Anforderung von Kyndryl wird der Lieferant rechtzeitig die Bedingungen seiner schriftlichen Verträge mit Unterauftragsverarbeitern und Subunternehmern hinsichtlich Datenschutz und Datensicherheit bereitstellen, einschließlich durch Bewilligung des Zugriffs auf die Verträge selbst, sofern der Lieferant dazu berechtigt ist.

1.3. Auf Anforderung von Kyndryl wird der Lieferant rechtzeitig Informationen über die Länder bereitstellen, in denen seine Waren und die Komponenten dieser Waren hergestellt, entwickelt oder anderweitig beschafft wurden.

2. Überprüfung (gemäß nachstehender Verwendung bezeichnet „Einrichtung“ einen physischen Standort, an dem der Lieferant Kyndryl Materialien hostet, verarbeitet oder anderweitig darauf zugreift)

2.1. Der Lieferant wird überprüfbare Aufzeichnungen führen, die die Einhaltung dieser Bedingungen nachweisen.

2.2. Kyndryl ist berechtigt, nach vorheriger schriftliche Benachrichtigung des Lieferanten unter Einhaltung einer Frist von 30 Tagen selbst oder mit einem externen Prüfer die Einhaltung dieser Bedingungen durch den Lieferanten zu überprüfen, einschließlich durch Besuch einer oder mehrerer Einrichtungen zu diesem Zweck. Kyndryl wird jedoch erst dann Rechenzentren besuchen, in denen der Lieferant Kyndryl Daten verarbeitet, wenn begründeter Grund zur Annahme besteht, dass dadurch sachdienliche Informationen gewonnen werden können. Der Lieferant wird an der Überprüfung durch Kyndryl mitwirken. Dies schließt die rechtzeitige und umfassende Reaktion auf Informationsanforderungen, z. B. über Dokumente, sonstige Aufzeichnungen, Befragungen relevanter Mitarbeiter des Lieferanten oder Ähnliches, ein. Der Lieferant kann Kyndryl Nachweise über die Einhaltung genehmigter Verhaltensregeln oder einer branchenüblichen Zertifizierung bereitstellen oder anderweitig Informationen bereitstellen, um die Einhaltung dieser Bedingungen nachzuweisen.

2.3. Eine Überprüfung darf innerhalb eines Zeitraums von 12 Monaten nur einmal stattfinden, es sei denn, (a) Kyndryl überprüft die Behebung von Problemen aus einer früheren Überprüfung innerhalb des Zeitraums von 12 Monaten oder (b) es ist eine Sicherheitsverletzung eingetreten und Kyndryl möchte die Einhaltung der für die Sicherheitsverletzung relevanten Verpflichtungen überprüfen. In jedem Fall wird Kyndryl eine vorherige schriftliche Benachrichtigung unter Einhaltung einer Frist von 30 Tagen gemäß den Angaben in Abschnitt 2.2 oben bereitstellen. Aufgrund der Dringlichkeit der Bearbeitung einer Sicherheitsverletzung kann jedoch die Durchführung einer Überprüfung durch Kyndryl nach einer kürzeren Frist als 30 Tagen erforderlich sein.

2.4. Eine Regulierungsbehörde oder ein sonstiger Verantwortlicher kann die Rechte wie Kyndryl gemäß Abschnitten 2.2 und 2.3 ausüben, wobei einer Regulierungsbehörde zusätzliche Rechte gemäß geltendem Recht zugestanden werden.

2.5. Sollte Kyndryl angemessenen Grund zur Annahme haben, dass der Lieferant diese Bedingungen nicht erfüllt (aufgrund einer Überprüfung im Rahmen dieser Bedingungen oder anderweitig), wird der Lieferant diese Nichterfüllung unverzüglich beheben.

3. Anti-Produktpiraterie-Programm

3.1. Falls die Waren des Lieferanten elektronische Komponenten (z. B. Festplattenlaufwerke, Solid-State-Laufwerke, Speicher, zentrale Verarbeitungseinheiten, logische Geräte oder Kabel) umfassen, verpflichtet sich der Lieferant, ein dokumentiertes Anti-Produktpiraterie-Programm zu pflegen und einzuhalten, um in erster Linie zu verhindern, dass Kyndryl Fälschungen von Komponenten bereitgestellt werden, und dann umgehend Fälle zu erkennen und zu beheben, in denen der Lieferant Kyndryl irrtümlicherweise Fälschungen von Komponenten bereitstellt. Der Lieferant wird diese Verpflichtung, ein dokumentiertes Anti-Produktpiraterie-Programm zu pflegen und einzuhalten, an seine Lieferanten weitergeben, die elektronische Komponenten bereitstellen, die in den Kyndryl bereitgestellten Waren des Lieferanten enthalten sind.

4. Fehlerbehebung

4.1. Wenn der Lieferant ihm obliegende Pflichten aus diesen Bedingungen nicht einhält und diese Nichteinhaltung zu einer Sicherheitsverletzung führt, wird der Lieferant den Fehler und die nachteiligen Auswirkungen der Sicherheitsverletzung nach den Weisungen und zeitlichen Vorgaben von Kyndryl beheben. Wenn die Sicherheitsverletzung jedoch auf die Bereitstellung eines gehosteten Multi-Tenant-Service durch den Lieferanten zurückzuführen ist und folglich viele Kunden des Lieferanten, einschließlich Kyndryl, betrifft, wird der Lieferant, in Anbetracht der Art der Sicherheitsverletzung, den Fehler und die nachteiligen Auswirkungen der Sicherheitsverletzung zeitnah und angemessen beheben und dabei alle Beiträge seitens Kyndryl zur Fehlerbehebung gebührend berücksichtigen.

4.2. Kyndryl hat das Recht, sich an der Behebung von Sicherheitsverletzungen, auf die in Abschnitt 4.1 verwiesen wird, zu beteiligen, wenn sie dies für angemessen oder notwendig hält, und der Lieferant trägt sämtliche Kosten und Ausgaben für seine Fehlerbehebung sowie die Kosten und Ausgaben für die Fehlerbehebung, die den Parteien durch eine solche Sicherheitsverletzung entstehen.

4.3. Kosten und Ausgaben für die Fehlerbehebung in Verbindung mit einer Sicherheitsverletzung könnten beispielsweise die Kosten und Ausgaben für die Erkennung und Untersuchung einer Sicherheitsverletzung, die Festlegung von Verantwortlichkeiten gemäß anwendbaren Gesetzen und Vorschriften, die Bereitstellung von Benachrichtigungen über Sicherheitsverletzungen, Einrichtung und Betrieb von Call-Centern, die Bereitstellung von Kontoüberwachungsservices und Services zur Wiederherstellung der Bonitätsbewertung, das erneute Laden von Daten, die Behebung von Produktfehlern (einschließlich durch Quellcode oder andere Entwicklungsmaßnahmen), die Bindung Dritter zur Unterstützung bei vorstehend genannten oder sonstigen relevanten Aktivitäten sowie sonstige Kosten und Ausgaben umfassen, die notwendig sind, um die nachteiligen Auswirkungen der Sicherheitsverletzung zu beheben. Kosten und Ausgaben umfassen weder entgangenen Gewinn, entgangene Geschäftsabschlüsse, Wertverlust oder Umsatzverlust, Schädigung des guten Rufs oder ausgebliebene Einsparungen von Kyndryl.