Artikel I, Geschäftskontaktinformationen („BCI“)

Dieser Artikel gilt, wenn der Lieferant oder Kyndryl die BCI des jeweils anderen verarbeitet.

1.1 Kyndryl und der Lieferant können die BCI des jeweils anderen überall dort verarbeiten, wo sie in Verbindung mit der Bereitstellung von Services und Liefergegenstände des Lieferanten geschäftlich tätig sind.

1.2 Eine Partei:

(a) wird die BCI der anderen Partei nicht für andere Zwecke verwenden oder offenlegen (zur Vermeidung von Missverständnissen: Keine der Parteien wird die BCI der anderen Partei verkaufen oder die BCI der anderen Partei für Marketingzwecke verwenden oder offenlegen, ohne dass die andere Partei vorher schriftlich zugestimmt hat und, falls erforderlich, die betroffene Person vorher schriftlich zugestimmt hat), und

(b) wird Informationen über die Verarbeitung der BCI der anderen Partei löschen, ändern, korrigieren, zurückgeben, als Information bereitstellen, die Verarbeitung der BCI der anderen Partei einschränken oder jede andere vernünftigerweise verlangte Maßnahme in Bezug auf die BCI der anderen Partei unverzüglich auf schriftliche Anfrage der anderen Partei durchführen, wann immer eine unbefugte Verwendung der personenbezogenen Daten eintritt und die Partei die Verarbeitung stoppen möchte und eine Korrektur verlangt.

1.3 Die Parteien gehen kein gemeinsames Verantwortungsverhältnis in Bezug auf die BCI der jeweils anderen Partei ein, und keine Bestimmung des Transaktionsdokuments ist so auszulegen, dass sie eine Absicht zur Begründung eines gemeinsamen Verantwortungsverhältnisses erkennen lässt.

1.4 Die Datenschutzerklärung von Kyndryl unter https://www.kyndryl.com/us/en/privacy enthält zusätzliche Details zur Verarbeitung von BCI durch Kyndryl.

1.5 Die Parteien haben technische und organisatorische Sicherheitsmaßnahmen implementiert und werden diese durchführen, um die BCI der anderen Partei gegen Verlust, Vernichtung, Veränderung, zufällige oder unbefugte Offenlegung, zufälligen oder unbefugten Zugriff und rechtswidrige Verarbeitung zu schützen.

1.6 Der Lieferant wird Kyndryl unverzüglich (in keinem Fall später als 48 Stunden) nach Bekanntwerden einer Sicherheitsverletzung, die das BCI von Kyndryl betrifft, benachrichtigen. Der Lieferant sendet eine solche Benachrichtigung an cyber.incidents@kyndryl.com. Der Lieferant wird Kyndryl in angemessener Weise Informationen über eine solche Verletzung und den Status etwaiger Korrektur- und Wiederherstellungsmaßnahmen des Lieferanten zur Verfügung stellen. Zu den vernünftigerweise angeforderten Informationen können beispielsweise Protokolle gehören, die den privilegierten, administrativen und sonstigen Zugriff auf Geräte, Systeme oder Anwendungen nachweisen. Darüber hinaus können forensische Bilder von Geräten, Systemen oder Anwendungen und andere ähnliche Elemente angefordert werden, soweit sie für die Sicherheitsverletzung oder die Korrektur- und Wiederherstellungsmaßnahmen des Lieferanten relevant sind.

1.7 Wenn der Lieferant nur die BCI von Kyndryl verarbeitet und keinen Zugriff auf andere Daten oder Materialien irgendeiner Art oder auf ein Unternehmenssystem von Kyndryl hat, sind dieser Artikel und Artikel X (Zusammenarbeit, Überprüfung und Korrektur) die einzigen Artikel, die für eine solche Verarbeitung gelten.

Artikel II, Technische und organisatorische Maßnahmen, Datensicherheit

Dieser Artikel gilt, wenn der Lieferant andere Kyndryl-Daten als die BCI von Kyndryl verarbeitet. Der Lieferant erfüllt die Anforderungen dieses Artikels bei der Bereitstellung aller Services und Liefergegenstände und schützt dadurch die Kyndryl-Daten vor Verlust, Vernichtung, Veränderung, zufälliger oder unbefugter Weitergabe, zufälligem oder unbefugtem Zugriff und rechtswidrigen Formen der Verarbeitung. Die Anforderungen dieses Artikels erstrecken sich auf alle IT-Anwendungen, Plattformen und Infrastruktur, die der Lieferant betreibt oder verwaltet, um Liefergegenstände und Services bereitzustellen. Dies schließt jegliche Entwicklungs-, Test-, Hosting-, Support-, Betriebs- und Rechenzentrumsumgebungen ein.

1. Datennutzung

1.1 Der Lieferant darf den Kyndryl-Daten ohne die vorherige schriftliche Einwilligung von Kyndryl keine anderen Informationen oder Daten hinzufügen oder in sie einbeziehen, was einschließlich personenbezogener Daten gilt. Der Lieferant darf Kyndryl-Daten in keinerlei Form, sei es zusammengefasst oder anderweitig, zu anderen Zwecken als der Bereitstellung von Services und Liefergegenständen verwenden oder wiederverwenden. (Beispielsweise darf der Lieferant Kyndryl-Daten nicht zur Bewertung der Effektivität von oder als Mittel zur Verbesserung der Angebote des Lieferanten, für Forschung und Entwicklung zur Erstellung neuer Angebote oder zur Erstellung von Berichten über die Angebote des Lieferanten verwenden oder wiederverwenden.) Sofern im Transaktionsdokument nicht ausdrücklich gestattet, ist es dem Lieferanten untersagt, Kyndryl-Daten zu verkaufen.

1.2 Der Lieferant bettet keine Web-Tracking-Technologien in die Liefergegenstände oder als Teile der Services ein (zu solchen Technologien gehören HTML5, lokale Speicherung, Drittanbieter-Tags oder -Token sowie Web-Beacons), es sei denn, dies ist ausdrücklich im Transaktionsdokument gestattet.

2. Anfragen Dritter und Vertraulichkeit

2.1 Der Lieferant legt Kyndryl-Daten keinem Dritten gegenüber offen, es sei denn, Kyndryl hat dies vorab schriftlich autorisiert. Wenn eine Behörde, einschließlich einer Regulierungsbehörde, Zugriff auf Kyndryl-Daten verlangt (z. B., wenn die US-Regierung dem Lieferanten eine Anweisung im Hinblick auf die nationale Sicherheit mit dem Ziel zustellt, ihr Kyndryl-Daten zu übermitteln), oder wenn eine Weitergabe von Kyndryl-Daten anderweitig gesetzlich vorgeschrieben ist, wird der Lieferant Kyndryl schriftlich über eine solche Anweisung oder Anforderung in Kenntnis setzen und Kyndryl eine angemessene Gelegenheit bieten, jede Offenlegung anzufechten. (Soweit eine Benachrichtigung gesetzlich verboten ist, wird der Lieferant die Schritte unternehmen, die er vernünftigerweise für angemessen hält, um gegen das Verbot und die Offenlegung von Kyndryl-Daten durch ein Gerichtsverfahren oder andere Mittel vorzugehen.)

2.2 Der Lieferant versichert Kyndryl, dass: (a) nur diejenigen seiner Mitarbeiter, die Zugriff auf Kyndryl-Daten für die Bereitstellung von Services oder Liefergegenständen benötigen, diesen Zugriff haben werden, und dann nur soweit dies für die Bereitstellung dieser Services und Liefergegenstände erforderlich ist; und (b) er seinen Mitarbeitern Vertraulichkeitsverpflichtungen auferlegt hat, die verlangen, dass diese Mitarbeiter Kyndryl-Daten nur im Rahmen dieser Bedingungen verwenden und nutzen.

3. **Rückgabe oder Löschung von Kyndryl-Daten**

3.1 Nach Wahl seitens Kyndryl löscht der Lieferant die Kyndryl-Daten bei Kündigung oder Ablauf des Transaktionsdokuments, oder früher auf Anfrage von Kyndryl, oder reicht sie an Kyndryl zurück. Soweit Kyndryl eine Löschung verlangt, macht der Lieferant, konsistent mit den Best Practices der Branche, die Daten unlesbar, sodass sie nicht mehr wieder zusammengefügt oder rekonstruiert werden können, und wird Kyndryl die Löschung bescheinigen. Wenn Kyndryl die Rückgabe von Kyndryl-Daten verlangt, so führt der Lieferant dies nach Kyndryls angemessenem Zeitplan und gemäß Kyndryls angemessenen schriftlichen Anweisungen aus.

Artikel III, Datenschutz

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

1. Verarbeitung

1.1 Kyndryl ernennt den Lieferanten zum Auftragsverarbeiter für die Verarbeitung personenbezogener Kyndryl-Daten zu dem alleinigen Zweck der Bereitstellung der Liefergegenstände und Services in Übereinstimmung mit den Anweisungen von Kyndryl, einschließlich derjenigen, die in diesen Bedingungen, dem Transaktionsdokument und der zugeordneten Basisvereinbarung zwischen den Parteien enthalten sind. Kommt der Lieferant einer Anweisung nicht nach, kann Kyndryl den betroffenen Teil der Services durch eine schriftliche Mitteilung kündigen. Wenn der Lieferant der Ansicht ist, dass eine Anweisung gegen ein Datenschutzgesetz verstößt, informiert der Lieferant Kyndryl unverzüglich und innerhalb des gesetzlich vorgeschriebenen Zeitrahmens über diesen Umstand. Wenn der Lieferant eine seiner Verpflichtungen aus diesen Bedingungen nicht einhält und dieses Versäumnis zu einer unbefugten Verwendung von personenbezogenen Daten führt, oder generell in jedem Fall einer unbefugten Nutzung von personenbezogenen Daten, hat Kyndryl das Recht, die Verarbeitung zu beenden und das Versäumnis zu korrigieren und die schädlichen Auswirkungen der unbefugten Nutzung zu beheben, wobei die Durchführung und Behebung nach angemessener Anweisung und Zeitplan von Kyndryl erfolgt.

1.2 Der Lieferant hält alle für die Services und Liefergegenstände geltenden Datenschutzgesetze ein.

1.3 Eine Anlage zum Transaktionsdokument oder das Transaktionsdokument selbst legt Folgendes in Bezug auf Kyndryl-Daten fest:

(a) Kategorien betroffener Personen;
(b) Arten personenbezogener Kyndryl-Daten;
(c) Datenaktionen und Verarbeitungsaktivitäten;
(d) Zeitraum und Häufigkeit der Verarbeitung; und
(e) eine Liste von Unterauftragsverarbeitern.

2. Technische und organisatorische Maßnahmen

2.1 Der Lieferant implementiert die technischen und organisatorischen Maßnahmen, die in Artikel II (Technische und organisatorische Maßnahmen, Datensicherheit) und Artikel VIII (Technische und organisatorische Maßnahmen, Allgemeine Sicherheit) festgelegt sind, und gewährleistet damit ein dem Risiko seiner Services und Liefergegenstände entsprechendes Sicherheitsniveau. Der Lieferant bestätigt und versteht die Beschränkungen in Artikel II, in diesem Artikel III und Artikel VIII, und wird sie einhalten.

3. Rechte und Anfragen betroffener Personen

3.1 Der Lieferant informiert Kyndryl unverzüglich (nach einem Zeitplan, der es Kyndryl und allen anderen Verantwortlichen ermöglicht, ihre gesetzlichen Verpflichtungen zu erfüllen) über jede Anfrage einer betroffenen Person, die Rechte einer betroffenen Person (z. B. Berichtigung, Löschung oder Blockung von Daten) in Bezug auf personenbezogene Kyndryl-Daten auszuüben. Der Lieferant kann eine betroffene Person, die eine solche Anfrage stellt, auch direkt an Kyndryl verweisen. Der Lieferant wird keine Anfragen von betroffenen Personen beantworten, es sei denn, er ist gesetzlich dazu verpflichtet oder wird von Kyndryl schriftlich dazu angewiesen.

3.2 Wenn Kyndryl verpflichtet ist, anderen für die Verarbeitung Verantwortlichen oder anderen Dritten (z. B. betroffenen Personen oder Aufsichtsbehörden) Informationen über personenbezogene Daten von Kyndryl zu übermitteln, unterstützt der Lieferant Kyndryl durch die Bereitstellung von Informationen und die Ergreifung anderer angemessener Maßnahmen, die Kyndryl anfordert, und zwar in einem Zeitplan, der es Kyndryl ermöglicht, diesen anderen für die Verarbeitung Verantwortlichen oder Dritten rechtzeitig zu antworten.

4. Unterauftragsverarbeiter

4.1 Der Lieferant lässt Kyndryl vorab eine schriftliche Mitteilung zukommen, bevor er einen neuen Unterauftragsverarbeiter beauftragt oder den Umfang der Verarbeitung durch einen vorhandenen Unterauftragsverarbeiter erweitert, wobei eine solche schriftliche Mitteilung den Namen des Unterauftragsverarbeiters ausweist und den neuen oder erweiterten Umfang der Verarbeitung beschreibt. Kyndryl kann einem solchen neuen Unterauftragsverarbeiter oder erweiterten Umfang aus angemessenen Gründen jederzeit ablehnen, und wenn dies der Fall ist, arbeiten die Parteien einvernehmlich zusammen, um sich mit der Ablehnung durch Kyndryl zu befassen. Vorbehaltlich des Rechts von Kyndryl, diese Maßnahme jederzeit abzulehnen, kann der Lieferant den neuen Unterauftragsverarbeiter beauftragen oder den Umfang der Verarbeitung des bestehenden Unterauftragsverarbeiters erweitern, falls Kyndryl nicht innerhalb von 30 Tagen nach dem Datum der schriftlichen Mitteilung des Lieferanten Einspruch erhebt.

4.2 Der Lieferant wird jedem zugelassenen Unterauftragsverarbeiter die Datenschutz-, Sicherheits- und Zertifizierungsverpflichtungen aus diesen Bedingungen auferlegen, bevor ein Unterauftragsverarbeiter Kyndryl-Daten verarbeitet. Der Lieferant haftet Kyndryl gegenüber in vollem Umfang für die Erfüllung der Verpflichtungen jedes Unterauftragsverarbeiters.

5. Grenzüberschreitende Datenverarbeitung

Wie unten verwendet:

Sicheres Drittland bezeichnet ein Land, das ein angemessenes Datenschutzniveau in Bezug auf die relevante Datenübermittlung gemäß den zutreffenden Datenschutzgesetzen oder Entscheidungen von Regulierungsbehörden bietet.

Datenimporteur bezeichnet entweder einen Auftragsverarbeiter oder einen Unterauftragsverarbeiter, der nicht in einem geeigneten Land ansässig ist.

EU-Standardvertragsklauseln („EU SCCs“) bezeichnet die EU-Standardvertragsklauseln (Entscheidung 2021/914 der Kommission) mit angewandten optionalen Klauseln, mit Ausnahme von Option 1 der Klausel 9(a) und Option 2 der Klausel 17, wie offiziell veröffentlicht unter https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

Serbische Standardvertragsklauseln („serbische SCCs“) bezeichnet die serbischen Standardvertragsklauseln, die vom „Serbischen Beauftragten für Informationen von öffentlicher Bedeutung und Schutz personenbezogener Daten“ angenommen wurden, wie veröffentlicht unter https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Standardvertragsklauseln („**SCCs**“) bezeichnet die Vertragsklauseln, die nach zutreffenden Datenschutzgesetzen für die Übermittlung personenbezogener Daten an Auftragsverarbeiter erforderlich sind, die nicht in sicheren Drittländern ansässig sind.

Zusatzvereinbarung des Vereinigten Königreichs zur internationalen Datenübermittlung zu den Standardvertragsklauseln der EU-Kommission („Zusatzvereinbarung des Vereinigten Königreichs“) bezeichnet die Zusatzvereinbarung des Vereinigten Königreichs für die internationale 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.

Zusatzvereinbarung zu den Standardvertragsklauseln der EU-Kommission, die die Schweiz betreffen („Schweizer Addendum“) bezeichnet die Vertragsklauseln zu den Standardvertragsklauseln der EU-Kommission, die gemäß dem Beschluss der Schweizer Datenschutzbehörde (**„FDPIC“**) und in

Übereinstimmung mit dem Schweizer Bundesgesetz über den Datenschutz (**„FADP“**) zur Anwendung kommen.

5.1 Der Lieferant übermittelt (auch nicht durch Fernzugriff) ohne die vorherige schriftliche Zustimmung von Kyndryl keine personenbezogenen Kyndryl-Daten über Grenzen hinweg oder legt solche Daten auf diese Weise offen. Wenn Kyndryl eine solche Einwilligung erteilt, koordinieren die Parteien, um die Einhaltung geltender Datenschutzgesetze sicherzustellen. Wenn SCCs nach diesen Gesetzen erforderlich sind, übernimmt der Lieferant auf Anfrage von Kyndryl die Standardvertragsklauseln.

5.2 Bezüglich EU-SCCs:

(a) Wenn der Lieferant nicht in einem sicheren Drittland ansässig ist: Der Lieferant übernimmt hiermit die EU-Standardvertragsklauseln als Datenimporteur für Kyndryl, und der Lieferant schließt mit jedem zugelassenen Unterauftragsverarbeiter schriftliche Vereinbarungen in Übereinstimmung mit Klausel 9 der EU-SCCs ab und liefert Kyndryl auf Anfrage Kopien dieser Vereinbarungen.

(i) Modul 1 der EU-SCCs kommt nicht zur Anwendung, soweit von den Parteien nichts anderes schriftlich vereinbart wurde.

(ii) Modul 2 der EU-SCCs kommt zur Anwendung, wenn Kyndryl ein Verantwortlicher ist, und Modul 3, wenn Kyndryl ein Auftragsverarbeiter ist. In Übereinstimmung mit Klausel 13 der EU-SCCs vereinbaren die Parteien, wenn die Module 2 oder 3 zur Anwendung kommen, dass (1) die EU-SCCs sich nach dem Gesetz desjenigen EU-Mitgliedstaats richten, in dem sich die zuständige Aufsichtsbehörde befindet, und (2) alle Streitigkeiten, die sich aus den EU-SCCs ergeben, vor den Gerichten desjenigen EU-Mitgliedstaats verhandelt werden, in dem sich die zuständige Aufsichtsbehörde befindet. Wenn ein solches Gesetz in (1) keine Begünstigtenrechte Dritter erlaubt, dann richten sich die EU-SCCs nach dem Recht der Niederlande, und alle Streitigkeiten, die sich aus den EU-SCCs gemäß (2) ergeben, werden vom zuständigen Gericht in Amsterdam, in den Niederlanden, beigelegt.

(b) Wenn beide Parteien, der Lieferant und Kyndryl, in einem sicheren Drittland ansässig sind, fungiert der Lieferant als Datenexporteur und schließt EU-SCCs mit jedem zugelassenen Unterauftragsverarbeiter in einem nicht sicheren Drittland ab. Der Lieferant führt das erforderliche Transfer Impact Assessment, TIA (Folgenabschätzung der Datenübermittlung) durch und benachrichtigt Kyndryl unverzüglich über (1) die eventuelle Notwendigkeit ergänzender Maßnahmen und (2) die angewandten Maßnahmen. Auf Anfrage liefert der Lieferant die TIA-Ergebnisse und alle zum Verständnis und zur Bewertung der Ergebnisse erforderlichen Informationen an Kyndryl. Falls Kyndryl mit den Ergebnissen des TIA des Lieferanten oder den angewandten ergänzenden Maßnahmen nicht einverstanden ist, koordinieren Kyndryl und der Lieferant, um eine zulässige Lösung zu finden. Kyndryl behält sich das Recht vor, betroffene Services des Lieferanten ohne Entschädigung auszusetzen oder zu kündigen. Zur Klarstellung: Dies entbindet die Unterauftragsverarbeiter des Lieferanten nicht von der Verpflichtung, die EU-SCCs in Bezug auf Kyndryl oder seinen Kunden einzuhalten, wie in Abschnitt 5.2 (d) unten beschrieben.

(c) Wenn der Lieferant im Europäischen Wirtschaftsraum ansässig ist und Kyndryl ein für die Verarbeitung Verantwortlicher ist, der nicht der Datenschutz-Grundverordnung 2016/679 unterliegt, dann gilt Modul 4 der EU-SCCs, und der Lieferant schließt hiermit die EU-SCCs als Datenexporteur mit Kyndryl ab. Wenn Modul 4 der EU-SCCs Anwendung findet, stimmen die Parteien überein, dass die EU-SCCs dem Recht der Niederlande unterliegen und alle Streitigkeiten, die sich aus den EU-SCCs ergeben, vor dem zuständigen Gericht in Amsterdam, den Niederlanden, beigelegt werden.

(d) Wenn andere Datenverantwortliche, wie z. B. Kunden oder verbundene Unternehmen, die Anfrage stellen, gemäß der „Kopplungsklausel“ in Klausel 7 eine Partei der EU-SCCs zu werden, stimmt der Lieferant hiermit einer solchen Anfrage zu.

(e) Technische und organisatorische Maßnahmen, die erforderlich sind, um den Anhang II der EU-SCCs auszufüllen, finden sich in diesen Bedingungen, dem Transaktionsdokument selbst und der zugeordneten Basisvereinbarung zwischen den Parteien.

(f) Im Falle eines Konflikts zwischen den EU-SCCs und diesen Bedingungen, haben die EU-SCCs Vorrang.

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

(a) Falls der Lieferant nicht in einem geeigneten Land ansässig ist: (i) schließt der Lieferant 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 Lieferant schriftliche Vereinbarungen mit jedem zugelassenen Unterverarbeiter ab und stellt Kyndryl auf Anfrage Kopien dieser Vereinbarungen zur Verfügung.

(b) Wenn der Lieferant 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 Lieferant 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 Informationen im Anhang (wie in Tabelle 3 aufgeführt) in der/den Zusatzvereinbarung(en) des Vereinigten Königreichs sind in den anwendbaren EU-SCCs, diesen Bedingungen, dem Transaktionsdokument selbst und der zugehörigen Basisvereinbarung 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 serbische SCCs:

(a) Wenn der Lieferant nicht in einem angemessenen Land ansässig ist: (i) schließt der Lieferant hiermit im eigenen Namen als Auftragsverarbeiter serbische SCCs mit Kyndryl ab; und (ii) schließt der Lieferant schriftliche Vereinbarungen mit jedem genehmigten Unterauftragsverarbeiter gemäß Artikel 8 der serbischen SCCs ab und stellt Kyndryl auf Anfrage Kopien dieser Vereinbarungen zur Verfügung.

(b) Wenn der Lieferant in einem geeigneten Land ansässig ist, schließt er hiermit im Namen jedes Unterauftragsverarbeiters, der in einem nicht geeigneten Land ansässig ist, serbische SCCs mit Kyndryl ab. Sollte der Lieferant nicht in der Lage sein, dies für einen solchen Unterauftragsverarbeiter zu tun, wird er Kyndryl die von diesem Unterauftragsverarbeiter unterzeichneten serbischen SCCs zur Gegenzeichnung durch Kyndryl vorlegen, bevor er dem Unterauftragsverarbeiter die Verarbeitung von Kyndryl personenbezogenen Daten gestattet.

(c) Je nach den Umständen dienen die serbischen SCCs zwischen Kyndryl und dem Lieferanten entweder als serbische SCCs zwischen einem Verantwortlichen und einem Auftragsverarbeiter oder als schriftliche Back-to-Back-Vereinbarung zwischen „Auftragsverarbeiter“ und „Unterauftragsverarbeiter“. Im Falle eines Konflikts zwischen den serbischen SCCs und diesen Bedingungen, haben die SCCs Vorrang.

(d) Informationen, die erforderlich sind, um die Anhänge 1 bis 8 der serbischen SCCs für den Zweck der Regelung der Übermittlung personenbezogener Daten in ein nicht sicheres Drittland zu erfüllen, können in diesen Bedingungen und im Anhang zum Transaktionsdokument oder im Transaktionsdokument selbst gefunden werden.

5.5. Zusatzvereinbarung(en), die die Schweiz betrifft/betreffen:

(a) Wenn und soweit ein Transfer personenbezogener Daten von Kyndryl gemäß Abschnitt 5.1. dem Schweizer Bundesgesetz über den Datenschutz („FADP “) unterliegt, sollen die vereinbarten EU-Standardvertragsklauseln aus Abschnitt 5.2 dieser Bedingungen den Transfer mit den folgenden Änderungen regeln, um der Norm DSGVO für personenbezogene Daten der Schweiz Rechnung zu tragen:

- Verweise auf die Datenschutzgrundverordnung („DSGVO") sind auch als Verweise auf die entsprechenden Bestimmungen des FADP zu verstehen,
- wobei zuständige Aufsichtsbehörde die Eidgenössische Datenschutz-Informationskommission gemäß Klausel 13 und Anhang I.C der EU SCCs ist.
- Im Fall, dass der Transfer ausschließlich dem FADP unterliegt, ist geltendes Recht das Recht der Schweiz, und
- der Begriff „Mitgliedstaat“ in Klausel 18 der EU-SCC wird auf die Schweiz ausgeweitet, um es Schweizer Datensubjekten zu ermöglichen, ihre Rechte an dem Ort ihres gewöhnlichen Aufenthalts wahrzunehmen.

(b) Zur Klarstellung: Keines der oben genannten Punkte soll das Datenschutzniveau der EU-SCCs in irgendeiner Weise schmälern, sondern nur dieses Schutzniveau auf Schweizer Datensubjekte ausweiten. Falls und soweit dies nicht der Fall ist, haben die EU-SCCs Vorrang.

6. Unterstützung und Aufzeichnungen

6.1 Unter Berücksichtigung der Art der Verarbeitung, unterstützt der Lieferant Kyndryl durch geeignete technische und organisatorische Maßnahmen zur Erfüllung der Verpflichtungen im Zusammenhang mit Anfragen und Rechten der betroffenen Personen. Der Lieferant unterstützt Kyndryl auch bei der Gewährleistung der Einhaltung von Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Meldung und Mitteilung einer Sicherheitsverletzung und die Erstellung von Datenschutz-Folgenabschätzungen, einschließlich der vorherigen Konsultation der zuständigen Aufsichtsbehörde, falls erforderlich, unter Berücksichtigung der dem Lieferanten zur Verfügung stehenden Informationen.

6.2 Der Lieferant pflegt aktuelle Unterlagen mit dem Namen und Kontaktinformationen jedes Unterauftragsverarbeiters, einschließlich des Vertreters und Datenschutzbeauftragten jedes Unterauftragsverarbeiters. Auf Anfrage stellt der Lieferant diese Unterlagen in einem Zeitplan zur Verfügung, der es Kyndryl erlaubt, rechtzeitig auf jede Nachfrage eines Kunden oder eines anderen Dritten zu reagieren.

Artikel IV, Technische und organisatorische Maßnahmen und Codesicherheit

Dieser Artikel gilt, wenn der Lieferant Zugriff auf den Kyndryl-Quellcode hat. Der Lieferant erfüllt die Voraussetzungen dieses Artikels und schützt dadurch den Kyndryl-Quellcode vor Verlust, Vernichtung, Veränderung, Änderung, zufälliger oder unbefugter Weitergabe, zufälligem oder unbefugtem Zugriff und rechtswidrigen Formen der Handhabung. Die Anforderungen dieses Artikels erstrecken sich auf alle IT-Anwendungen, -Plattformen und -Infrastrukturen, die der Lieferant bei der Erbringung von Lieferungen und Leistungen und bei der Handhabung der Technologie von Kyndryl betreibt oder verwaltet. Das schließt alle Entwicklungs-, Test-, Hosting-, Support-, Betriebs- und Rechenzentrumsumgebungen ein.

1. Sicherheitsanforderungen

Wie unten angegeben:

Verbotenes Land jedes Land, (a) das von der US-Regierung im Rahmen der Executive Order vom 15. Mai 2019 über die Sicherung der Lieferkette für Informations- und Kommunikationstechnologie und Services als ausländischer Gegner bezeichnet wurde, das (b) in Übereinstimmung mit Abschnitt 1654 des U.S. National Defense Authorization Act (US-amerikanischen Nationalen Verteidigungsgenehmigungsgesetzes) von 2019 aufgeführt ist oder (c) das im Transaktionsdokument als „verbotenes Land“ bezeichnet wird.

1.1 Der Lieferant vermarktet oder übereignet keinen Kyndryl-Quellcode treuhänderisch für den erzielbarer Nutzen eines Dritten.

1.2 Der Lieferant wird nicht zulassen, dass ein Kyndryl-Quellcode auf Servern in einem verbotenen Land gespeichert wird.Der Lieferant erlaubt niemandem, einschließlich seines Personals, das sich in einem verbotenen Land befindet oder ein verbotenes Land besucht (für die Dauer eines solchen Besuchs), aus irgendeinem Grund auf einen Kyndryl-Quellcode zuzugreifen oder ihn zu verwenden. Dies gilt unabhängig davon, wo sich dieser Kyndryl-Quellcode irgendwo auf der Welt befindet. Weiter gestattet der Lieferant nicht, dass Entwicklungs-, Test- oder eine andere Arbeiten in einem verbotenen Land durchgeführt werden, die einen solchen Zugriff oder eine solche Verwendung erforderlich machen würden.

1.3 Der Lieferant bringt oder vermarktet einen Kyndryl-Quellcode nicht in einen rechtlichen Zuständigkeitsbereich, in dem Gesetze oder die Rechtsauslegung die Offenlegung des Quellcodes an Dritte verlangt. Wenn es in einem rechtlichen Zuständigkeitsbereich, in dem sich der Kyndryl-Quellcode befindet, zu einer Gesetzesänderung oder Änderung der Interpretation eines Gesetzes kommt, die dazu führen kann, dass der Lieferant verpflichtet ist, einen Quellcode Dritten gegenüber offenzulegen, vernichtet der Lieferant unverzüglich diesen Kyndryl-Quellcode oder entfernt ihn aus dem rechtlichen Zuständigkeitsbereich. Er bringt keinen Kyndryl-Quellcode in diesen rechtlichen Zuständigkeitsbereich, so lange dieses Gesetz oder diese Rechtsauslegung Bestand hat.

1.4 Der Lieferant wird weder direkt noch indirekt Maßnahmen ergreifen, einschließlich des Abschlusses von Verträgen, die dazu führen könnten, dass der Lieferant, Kyndryl oder ein Dritter einer Offenlegungspflicht gemäß den Abschnitten 1654 oder 1655 des U.S. National Defense Authorization Act von 2019 unterliegen würden. Zur Vermeidung von Missverständnissen: Außer wie ausdrücklich im Transaktionsdokument oder der zugeordneten Basisvereinbarung zwischen den Parteien erlaubt, ist es dem Lieferanten unter keinen Umständen ohne vorherige schriftliche Einwilligung von Kyndryl gestattet, einen Kyndryl-Quellcode einem Dritten gegenüber offenzulegen.

1.5 Wenn Kyndryl den Lieferanten benachrichtigt oder eine dritte Partei eine der Parteien benachrichtigt, dass: (a) der Lieferant es zugelassen hat, dass ein Kyndryl-Quellcode in ein verbotenes Land oder in eine Gerichtsbarkeit im Sinne von Abschnitt 1.3 gebracht wurde, (b) der Lieferant den Kyndryl-Quellcode auf andere Weise freigegeben, auf ihn zugegriffen oder ihn in einer Weise verwendet hat, die nicht durch das Transaktionsdokument oder die Basisvereinbarung oder eine sonstige Vereinbarung zwischen den Parteien gestattet ist, oder (c) der Lieferant gegen obigen Abschnitt 1.4 verstoßen hat, so gilt unbeschadet der Rechte von Kyndryl, gegen eine solche Nichteinhaltung gerichtlich oder nach Ermessen oder gemäß dem Transaktionsdokument oder der zugehörigen Basis oder einer anderen Vereinbarung zwischen den Parteien vorzugehen: (i) wenn eine solche Mitteilung an den Lieferanten erfolgt, wird der Lieferant die Mitteilung

unverzüglich an Kyndryl weiterleiten; und (ii) der Lieferant wird auf angemessene Anweisung von Kyndryl die Angelegenheit nach dem von Kyndryl (nach Rücksprache mit dem Lieferanten) angemessen festgelegten Zeitplan untersuchen und berichtigen.

1.6 Wenn Kyndryl vernünftigerweise annimmt, dass Änderungen an den Richtlinien, Verfahren, Kontrollinstrumenten oder Praktiken des Lieferanten in Bezug auf den Quellcode-Zugriff erforderlich sein können, um gegen eine Verletzung der Cybersicherheit, des Diebstahls von geistigem Eigentum oder ähnliche oder verwandte Risiken vorzugehen (einschließlich des Risikos, dass Kyndryl ohne solche Änderungen im Verkauf an bestimmte Kunden oder in bestimmte Märkte eingeschränkt werden oder anderweitig nicht in der Lage sein könnte, die Sicherheits- oder Supply-Chain-Anforderungen des Kunden zu erfüllen), kann Kyndryl sich an den Lieferanten wenden, um die Maßnahmen zu besprechen, die für ein Vorgehen gegen solche Risiken erforderlich sind, was auch für Änderungen an solchen Richtlinien, Verfahren, Kontrollinstrumenten oder Praktiken gilt. Auf Anfrage von Kyndryl koordiniert der Lieferant mit Kyndryl, um zu prüfen, ob solche Änderungen erforderlich sind, und um angemessene Änderungen im beiderseitigen Einvernehmen umzusetzen.

Artikel V, Sichere Entwicklung

Dieser Artikel kommt zur Anwendung, wenn der Lieferant Kyndryl seinen Quellcode oder den anderer Anbieter oder On-Premise-Software zur Verfügung stellt, oder wenn Liefergegenstände oder Services des Lieferanten für einen Kunden von Kyndryl als Teil eines Kyndryl-Produkts oder Kyndryl-Services bereitgestellt werden.

1. Sicherheitsbereitschaft

1.1 Der Lieferant benutzt die internen Kyndryl-Prozesse, die die Sicherheitsbereitschaft von Kyndryl-Produkten und -Services beurteilen, die von den Liefergegenständen des Lieferanten abhängig sind, was auch die rechtzeitige und vollständige Beantwortung von Anfragen nach Informationen, unbeachtlich ob in Form von Dokumenten, anderen Aufzeichnungen, Interviews mit dem relevanten Personal des Lieferanten oder dergleichen, einschließt.

2. Sichere Entwicklung

2.1 Dieser Abschnitt 2 gilt nur, wenn der Lieferant für Kyndryl On-Premise-Software bereitstellt.

2.2 Der Lieferant hat in Übereinstimmung mit Best Practices der Branche das Netzwerk, die Plattform, das System, die Anwendung, das Gerät, die physische Infrastruktur, die Incident-Response und auf das Personal ausgerichtete Sicherheitsrichtlinien, -verfahren und -kontrollinstrumente implementiert und wird diese während der gesamten Laufzeit des Transaktionsdokument aufrechterhalten, die notwendig sind, um (a) die Entwicklungs-, Aufbau-, Test- und Betriebssysteme und -umgebungen, die der Lieferant oder ein vom Lieferanten beauftragter Dritter betreibt, verwaltet, nutzt oder sich anderweitig darauf oder in Bezug auf die Liefergegenstände verlässt, und um (b) alle Quellcodes in Liefergegenständen gegen Verlust, rechtswidrige Formen der Handhabung und unbefugten Zugriff, unbefugte Offenlegung oder Veränderung zu schützen.

3. ISO 20243-Zertifizierung

3.1 Dieser Abschnitt 3 gilt nur, wenn Liefergegenstände oder Services des Lieferanten für einen Kyndryl-Kunden als Teil eines Kyndryl-Produkts oder Kyndryl-Services bereitgestellt werden.

3.2 Der Lieferant besorgt sich eine Bescheinigung der Konformität mit ISO/IEC 20243 „Informationstechnologie, Offener vertrauenswürdiger Technologieanbieter, TM-Standard (O-TTPS), Entschärfung böswillig gefälschter und nachgeahmter Produkte“ (entweder eine Eigenbescheinigung oder eine, die auf der Grundlage der Bewertung eines seriösen externen Prüfers beruht). Alternativ holt der Lieferant, wenn er schriftlich darum anfragt und Kyndryl dem schriftlich zustimmt, eine Bescheinigung der Konformität mit einem im wesentlichen gleichen Industriestandard ein, der sich mit den Praktiken der sicheren Entwicklung

und Supply-Chain-Praktiken befasst (entweder eine Eigenbescheinigung oder eine, die auf der Grundlage der Bewertung eines renommierten externen Prüfers beruht, sofern und wie Kyndryl dem zustimmt).

3.3 Der Lieferant holt die Bescheinigung der Konformität mit ISO 20243 oder mit einem im wesentlichen gleichen Industriestandard (falls Kyndryl dem schriftlich zustimmt) innerhalb von 180 Tage nach dem Datum des Inkrafttretens des Transaktionsdokuments ein
und erneuert die Bescheinigung danach alle 12 Monate (bei jeder Erneuerung im Vergleich mit der jeweils aktuellsten Version des betreffenden Standards, d. h. ISO 20243 oder, sofern Kyndryl dies schriftlich genehmigt hat, mit einem im wesentlichen gleichen Industriestandard, der sich mit den Praktiken der sicheren Entwicklung und Supply-Chain-Praktiken befasst).

3.4 Der Lieferant stellt Kyndryl auf Anfrage unverzüglich eine Kopie der Bescheinigungen bereit, die der Lieferant gemäß den Abschnitten 2.1 und 2.2 oben einzuholen verpflichtet ist.

4. Sicherheitslücken

Wie unten angegeben:

Fehlerkorrektur bezeichnet Fehlerkorrekturen und Überarbeitungen, die Fehler oder Mängel, einschließlich Sicherheitslücken, in Liefergegenständen beheben.

Risikominderung bezeichnet alle bekannten Mittel zur Verringerung oder Vermeidung der Risiken einer Sicherheitslücke.

Sicherheitslücke bezeichnet einen Zustand im Design, in der Codierung, Entwicklung, Implementierung, im Test, Betrieb, Support, in der Wartung oder der Verwaltung eines Liefergegenstandes, der einen Angriff durch jemanden zulässt, der zu einem unbefugten Zugriff oder zu einer Ausnutzung führen könnte. Hierin eingeschlossen sind: (a) Zugriff auf, Kontrolle oder Unterbrechung des Betriebs eines Systems, (b) Zugriff auf, Löschung, Veränderung oder Extraktion von Daten oder (c) Änderungen der Identität, von Befugnissen oder Berechtigungen von Benutzern oder Administratoren. Eine Sicherheitslücke kann unabhängig davon bestehen, ob ihr eine CVE-ID (Common Vulnerabilities and Exposures/Häufige Schwachstellen und Gefährdungen), ein Scoring oder eine offizielle Klassifikation zugewiesen ist oder nicht.

4.1 Der Lieferant sichert zu und garantiert, dass er: (a) Best Practices der Branche nutzt, um Sicherheitslücken zu identifizieren, u. a. durch kontinuierliche statische und dynamische Scans der Quellcode-Anwendungssicherheit, Scans der Open-Source-Sicherheit und Scans auf Systemlücken, und (b) die Anforderungen dieser Bedingungen einhält, um dazu beizutragen, Sicherheitslücken in Liefergegenständen und in allen IT- Anwendungen, -Plattformen und -Infrastrukturen zu verhindern, zu erkennen und zu beseitigen, in denen und durch die der Lieferant Services und Liefergegenstände erstellt und bereitstellt.

4.2 Wenn dem Lieferanten eine Sicherheitslücke in einem Liefergegenstand oder einer solchen IT-Anwendung, Plattform oder Infrastruktur bekannt wird, stellt der Lieferant für Kyndryl eine Fehlerkorrektur und Schadensbegrenzung für alle Versionen und Releases der Liefergegenstände in Übereinstimmung mit den Schweregraden und Zeitrahmen bereit, die in den folgenden Tabellen definiert sind:

Schweregrad*
Gefährliche Sicherheitslücke – ist eine Sicherheitslücke, die eine schwerwiegende und potenziell globale Bedrohung darstellt. Kyndryl bestimmt gefährliche Sicherheitslücken nach eigenem Ermessen, unabhängig vom CVSS-Basisscore
Kritisch – ist eine Sicherheitslücke mit einem CVSS-Basisscore von 9 bis 10,0
Hoch – ist eine Sicherheitslücke mit einem CVSS-Basisscore von 7,0 bis 8,9
Mittel – ist eine Sicherheitslücke mit einem CVSS-Basisscore von 4,0 bis 6,9
Niedrig – ist eine Sicherheitslücke mit einem CVSS-Basisscore von 0,0 bis 3,9

Zeitrahmen				
Gefahr	***Kritisch***	***Hoch***	***Mittel***	***Niedrig***
4 Tage oder weniger, wie vom Chief Information Security Office von Kyndryl festgelegt	30 Tage	30 Tage	90 Tage	Gemäß Best Practices der Branche

* In allen Fällen, in denen einer Sicherheitslücke kein CVSS-Basisscore zugewiesen werden kann, wendet der Lieferant einen Schweregrad an, der der Art und den Umständen dieser Sicherheitslücke angemessen ist.

4.3 Für eine Sicherheitslücke, die öffentlich bekannt gegeben wurde und für die der Lieferant noch keine Fehlerkorrektur oder -minderung bereitgestellt hat, implementiert der Lieferant alle technisch durchführbaren zusätzlichen Sicherheitsmaßnahmen, mit denen die Risiken der Verletzlichkeit gemindert werden können.

4.4 Wenn Kyndryl mit der Intervention des Lieferanten in Bezug auf eine Sicherheitslücke in einem Liefergegenstand oder einer oben referenzierten Anwendung, Plattform oder Infrastruktur unzufrieden ist, arrangiert der Lieferant für Kyndryl, unbeschadet anderer Rechte von Kyndryl, unverzüglich eine Möglichkeit, um seine Bedenken direkt mit dem stellvertretenden Vorsitzenden des Lieferanten oder einem vergleichbaren Entscheidungsträger zu besprechen, der für die Bereitstellung der Fehlerkorrektur verantwortlich ist.

4.5 Beispiele für Sicherheitslücken sind Codes von Drittanbietern oder End-of-Service (EOS) Open-Source-Codes, bei denen diese Arten von Codes keine Sicherheitsupdates mehr erhalten.

Artikel VI, Zugriff auf Unternehmenssysteme

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

1. Allgemeine Bedingungen

1.1 Kyndryl bestimmt, ob Mitarbeiter des Lieferanten Zugriff auf Unternehmenssysteme erhalten sollen. Wenn Kyndryl dies autorisiert, wird der Lieferant die Anforderungen dieses Artikels erfüllen und seine Mitarbeiter mit einem solchen Zugriff dazu veranlassen, diese ebenfalls zu erfüllen.

1.2 Kyndryl wird die Mittel bestimmten, mit denen Mitarbeiter des Lieferanten auf Unternehmenssysteme zugreifen dürfen, einschließlich der Frage, ob diese Mitarbeiter über von Kyndryl oder vom Lieferanten bereitgestellte Geräte auf Unternehmenssysteme zugreifen sollen oder nicht.

1.3 Mitarbeiter des Lieferanten dürfen nur auf Unternehmenssysteme zugreifen und nur die Geräte verwenden, die Kyndryl für den Zugriff im Hinblick auf die Bereitstellung von Services freigibt. Mitarbeiter des Lieferanten dürfen die Geräte, die Kyndryl so freigegeben hat, nicht dazu verwenden, Services für andere Personen oder Unternehmen bereitzustellen oder um auf IT-Systeme, Netzwerke, Anwendungen, Websites, E-Mail-Tools, Tools für die Zusammenarbeit oder dergleichen für oder in Verbindung mit den Services zuzugreifen.

1.4 Zur Vermeidung von Missverständnissen: Die Mitarbeiter des Lieferanten dürfen die Geräte, die Kyndryl für den Zugriff auf Unternehmenssysteme freigegeben hat, nicht für persönliche Gründe nutzen (z. B. dürfen die Mitarbeiter des Lieferanten keine persönlichen Dateien wie Musik, Videos, Bilder oder andere Elemente auf solchen Geräten speichern und das Internet nicht von solchen Geräten aus für private Gründe nutzen).

1.5 Mitarbeiter des Lieferanten dürfen ohne Kyndryls vorherige schriftliche Genehmigung keine Kyndryl-Materialien kopieren, auf die über ein Unternehmenssystem zugegriffen werden kann (und dürfen niemals Kyndryl-Materialien auf eine mobile Speichereinheit, wie z. B. einen USB, eine externe Festplatte oder andere ähnliche Elemente kopieren).

1.6 Auf Anfrage bestätigt der Lieferant, unter Angabe des Mitarbeiternamens, die bestimmten Unternehmenssysteme, auf die seine Mitarbeiter zugreifen dürfen, und darauf in einem von Kyndryl angegebenen Zeitraum zugegriffen haben.

1.7 Der Lieferant benachrichtigt Kyndryl innerhalb von vierundzwanzig (24) Stunden, nachdem ein Mitarbeiter des Lieferanten, der Zugriff auf ein Unternehmenssystem hat, nicht mehr: (a) beim Lieferanten beschäftigt ist oder (b) an Aktivitäten tätig ist, die einen solchen Zugriff erfordern. Der Lieferant koordiniert mit Kyndryl, um sicherstellen, dass der Zugriff für solche ehemaligen oder aktuellen Mitarbeiter unverzüglich widerrufen wird.

1.8 Der Lieferant meldet alle tatsächlichen oder vermuteten Sicherheitsvorfälle (wie z. B. Verlust eines Geräts von Kyndryl oder des Lieferanten oder den unbefugten Zugriff auf so ein Gerät oder Daten, Materialien oder andere Informationen jeglicher Art) an Kyndryl und koordiniert mit Kyndryl bei der Untersuchung solcher Vorfälle.

1.9 Der Lieferant darf keinem Beauftragten, unabhängigen Auftragnehmer oder Mitarbeiter eines Subunternehmers ohne vorherige schriftliche Zustimmung von Kyndryl den Zugang zu einem Unternehmenssystem gestatten. Wenn Kyndryl diese Zustimmung erteilt, verpflichtet der Lieferant diese Personen und ihre Arbeitgeber vertraglich zur Einhaltung der Anforderungen dieses Artikels, als wären diese Personen Mitarbeiter des Lieferanten, und ist gegenüber Kyndryl für alle Handlungen und Unterlassungen einer solchen Person oder eines solchen Arbeitgebers in Bezug auf den Zugang zum Unternehmenssystem verantwortlich.

2. Gerätesoftware

2.1 Der Lieferant wird seine Mitarbeiter anweisen, rechtzeitig alle Gerätesoftware zu installieren, die Kyndryl benötigt, um den Zugang zu den Unternehmenssystemen auf sichere Art und Weise zu ermöglichen. Weder der Lieferant noch seine Mitarbeiter werden den Betrieb dieser Software oder der Sicherheitsfunktionen stören, die die Software ermöglicht.

2.2 Der Lieferant und seine Mitarbeiter beachten die von Kyndryl festgelegten Regeln zur Gerätekonfiguration. Sie koordinieren mit Kyndryl, um sicherzustellen, dass die Software so funktioniert, wie Kyndryl dies beabsichtigt. Der setzt beispielsweise keine Softwarefunktionen zur Blockierung von Websites oder automatisierte Patching-Funktionen außer Kraft.

2.3 Mitarbeiter des Lieferanten dürfen die Geräte, die sie für den Zugriff auf Unternehmenssysteme verwenden, oder ihre Benutzernamen, Passwörter für ihr Gerät oder dergleichen nicht mit anderen Personen teilen.

2.4 Wenn Kyndryl-Mitarbeiter des Lieferanten autorisiert, auf Unternehmenssysteme unter Verwendung von Lieferantengeräten zuzugreifen, installiert der Lieferant ein Betriebssystem auf den von Kyndryl freigegebenen Geräten, lässt es dort ausführen, und führt innerhalb einer angemessenen Zeit nach entsprechender Anweisung von Kyndryl ein Upgrade auf eine neue Version dieses Betriebssystems oder auf ein neues Betriebssystem durch.

3. Beaufsichtigung und Mitwirkungsleistungen

3.1 Kyndryl hat das uneingeschränkte Recht, potenzielle unbefugte Zugriffe und andere Angriffe auf die Cybersicherheit, ohne vorherige Benachrichtigung des Lieferanten oder eines seiner Mitarbeiter oder anderer Personen, in beliebiger Weise, von beliebigen Orten aus und mit allen Mitteln zu überwachen und zu korrigieren, die Kyndryl für notwendig oder angemessen hält. Unter dieses Recht fällt beispielsweise, dass Kyndryl zu jeder Zeit (a) einen Sicherheitstest auf jedem beliebigen Gerät durchführen kann, (b) durch technische oder andere Mittel Kommunikation (einschließlich der E-Mail von beliebigen E-Mail-Konten), Aufzeichnungen, Dateien und andere Elemente, die auf einem beliebigen Gerät gespeichert oder über ein Unternehmenssystem übertragen werden, überwachen, wiederherstellen und überprüfen kann, und (c) von jedem Gerät eine vollständige forensische Sicherung erstellen kann. Wenn Kyndryl zur Ausübung seiner Rechte die Mitwirkung des Lieferanten benötigt, wird der Lieferant den Aufforderungen von Kyndryl zur Mitwirkung vollständig und rechtzeitig nachkommen (einschließlich beispielsweise der Aufforderung, ein Gerät sicher zu konfigurieren, Überwachungs- oder andere Software auf einem Gerät zu installieren, Verbindungsdetails auf Systemebene mitzuteilen, Maßnahmen zur Reaktion auf einen Vorfall auf einem Gerät zu ergreifen und Kyndryl physischen Zugang zu einem Gerät zu gewähren, um ein vollständiges forensisches Bild zu erhalten oder ähnliches und damit verbundene Aufforderungen).

3.2 Kyndryl kann für jeden oder alle Mitarbeiter des Lieferanten den Zugriff auf Unternehmenssysteme ohne vorherige Benachrichtigung des Lieferanten oder eines oder aller Mitarbeiter des Lieferanten oder anderer widerrufen, wenn Kyndryl zur Ansicht gelangt, dass dies zum Schutz von Kyndryl erforderlich ist.

3.3 Die Rechte von Kyndryl werden durch keine Bestimmung des Transaktionsdokuments, der zugeordneten Basisvereinbarung zwischen den Parteien oder einer anderen Vereinbarung zwischen den Parteien, einschließlich keiner solcher Bestimmungen in irgendeiner Weise blockiert, vermindert oder eingeschränkt, die es erforderlich machen können, dass Daten, Materialien oder andere Informationen irgendeiner Art nur an einem bestimmten Standort oder an bestimmten Standorten gespeichert werden, oder dass nur Personen von einem bestimmten Standort oder von bestimmten Standorten Zugriff auf solche Daten, Materialien oder andere Informationen haben.

4. Kyndryl-Geräte

4.1 Kyndryl behält den Rechtsanspruch auf alle Kyndryl-Geräte, wobei der Lieferant das Verlustrisiko für die Geräte, einschließlich eines solchen wegen Diebstahl, Vandalismus oder Vernachlässigung trägt. Der Lieferant wird ohne die vorherige schriftliche Zustimmung von Kyndryl keine Änderungen an Kyndryl-Geräten vornehmen oder zulassen, wobei eine Änderung jede Änderung an einem Gerät ist, einschließlich jeder Änderung der Gerätesoftware, der Anwendungen, des Sicherheitsdesigns, der Sicherheitskonfiguration oder des physischen, mechanischen oder elektrischen Designs.

4.2 Der Lieferant reicht alle Kyndryl-Geräte innerhalb von 5 Geschäftstagen zurück, nachdem die Notwendigkeit endet, dass mit diesen Geräten Services bereitgestellt werden. Wenn Kyndryl es verlangt, vernichtet der Lieferant gleichzeitig alle Daten, Materialien und sonstigen Informationen jeglicher Art auf diesen Geräten, ohne dabei irgendwelche Kopien zu behalten, wobei er für die dauerhafte Löschung aller dieser Daten, Materialien und anderen Informationen die Best Practices der Branche befolgt. Der Lieferant verpackt und liefert Kyndryl-Geräte im gleichen Zustand, wie sie an den Lieferanten geliefert wurden, auf eigene Kosten an den von Kyndryl genannten Standort zurück. In Bezug auf den Zustand ist eine übliche technisch bedingte Wertminderung akzeptabel. Die Nichteinhaltung einer Verpflichtung aus diesem Abschnitt 4.2 durch den Lieferanten stellt eine wesentliche Vertragsverletzung des Transaktionsdokuments und der zugeordneten Basisvereinbarung sowie eventueller zugehöriger Vereinbarungen zwischen den Parteien dar. Dabei wird vorausgesetzt, dass eine Vereinbarung „zugehörig“ ist, wenn der Zugriff auf ein Unternehmenssystem im Rahmen dieser Vereinbarung die Aufgaben oder andere Aktivitäten des Lieferanten erleichtert.

4.3 Kyndryl bietet Support für Kyndryl-Geräte (einschließlich Geräteinspektion und vorbeugender und abhelfender Wartung). Der Lieferant informiert Kyndryl unverzüglich über die Notwendigkeit von Abhilfemaßnahmen.

4.4. Für Softwareprogramme, die Kyndryl besitzt oder zu deren Lizenzierung Kyndryl berechtigt ist, gewährt Kyndryl dem Lieferanten ein vorläufiges Recht zur Nutzung, Speicherung und Anfertigung ausreichender Kopien, um seine berechtigte Nutzung von Kyndryl-Geräten zu unterstützen. Der Lieferant darf Programme nicht an Dritte übertragen, Kopien von Softwarelizenzinformationen anfertigen oder Programme disassemblieren, dekompilieren, rückentwickeln oder anderweitig übersetzen, es sei denn, dies ist ausdrücklich auf Grund von geltendem Recht ohne die Möglichkeit eines vertraglichen Verzichts zulässig.

5. Aktualisierungen

5.1 Ungeachtet gegenteiliger Bestimmungen im Transaktionsdokument oder der zugeordneten Basisvereinbarung zwischen den Parteien, kann Kyndryl nach schriftlicher Mitteilung an den Lieferanten und ohne die Notwendigkeit einer Zustimmung des Lieferanten diesen Artikel aktualisieren, ergänzen oder anderweitig erweitern, um Anforderungen nach geltendem Recht oder aus einer Verpflichtung des Kunden mit dem Ziel zu erfüllen, Entwicklungen in Best Practices zu Sicherheitsfragen oder in sonstiger Form abzubilden, wie dies Kyndryl für notwendig hält, um Unternehmenssysteme oder Kyndryl zu schützen.

Artikel VII, Personalverstärkung

Dieser Artikel gilt, wenn die Mitarbeiter des Lieferanten ihre gesamte Arbeitszeit der Bereitstellung von Services für Kyndryl aufwenden, all diese Services in Räumlichkeiten von Kyndryl, Räumlichkeiten des Kunden oder von zu Hause aus erbringen und nur Services unter Verwendung von Kyndryl-Geräten bereitstellen, um auf Unternehmenssysteme zuzugreifen.

1. Zugriff auf Unternehmenssysteme; Kyndryls Umgebungen

1.1 Der Lieferant darf Services nur durch den Zugriff auf Unternehmenssysteme unter Verwendung von Geräten erbringen, die Kyndryl bereitstellt.

1.2 Der Lieferant hält für alle Zugriffe auf Unternehmenssysteme die Bedingungen aus Artikel VI (Zugriff auf Unternehmenssysteme) ein.

1.3 Von Kyndryl bereitgestellte Geräte sind die einzigen Geräte, die der Lieferant und seine Mitarbeiter verwenden dürfen, um Services zu erbringen, und dürfen nur vom Lieferanten und seinen Mitarbeitern verwendet werden, um Services zu erbringen. Zur Vermeidung von Missverständnissen: Der Lieferant oder seine Mitarbeiter dürfen für die Erbringung von Services keinesfalls andere Geräte verwenden oder Kyndryl-Geräte für andere Auftraggeber des Lieferanten oder für andere Zwecke als die Erbringung von Services für Kyndryl verwenden.

1.4 Mitarbeiter des Lieferanten, die Kyndryl-Geräte verwenden, dürfen Kyndryl-Materialien miteinander teilen und solche Materialien auf Kyndryl-Geräten speichern, jedoch nur in dem begrenzten Umfang, also nur, wenn Teilen und Speichern für die erfolgreiche Erbringung der Services erforderlich sind.

1.5 Außer für eine solche Speicherung auf Kyndryl-Geräten dürfen der Lieferant oder seine Mitarbeiter unter keinen Umständen Kyndryl-Materialien aus Kyndryls Repositories, Umgebungen, Tools oder Infrastrukturen entfernen, wo sie von Kyndryl aufbewahrt werden.

1.6 Zur Vermeidung von Missverständnissen: Der Lieferant und seine Mitarbeiter sind nicht autorisiert, Kyndryl-Materialien ohne Kyndryls vorherige schriftliche Zustimmung in Repositories, Umgebungen, Tools oder Infrastrukturen oder andere Systeme, Plattformen, Netzwerke oder dergleichen des Lieferanten zu übertragen.

1.7 Artikel VIII (Technische und organisatorische Maßnahmen, Allgemeine Sicherheit) gilt nicht für die Services des Lieferanten, sofern die Mitarbeiter des Lieferanten ihre gesamte Arbeitszeit für die Bereitstellung von Services für Kyndryl aufwenden, all diese Services in Räumlichkeiten von Kyndryl, Räumlichkeiten des Kunden oder von zu Hause aus erbringen und nur Services unter Verwendung von Kyndryl-Geräten bereitstellen, um auf Unternehmenssysteme zuzugreifen. Ansonsten gilt Artikel VIII für die Services des Lieferanten.

Artikel VIII, Technische und organisatorische Maßnahmen, Allgemeine Sicherheit

Dieser Artikel findet Anwendung, wenn der Lieferant Services oder Liefergegenstände für Kyndryl erbringt, es sei denn, der Lieferant hat bei der Bereitstellung dieser Services und Liefergegenstände nur Zugriff auf Kyndryl BCI (d. h. der Lieferant verarbeitet keine anderen Kyndryl-Daten und hat keinen Zugriff auf andere Kyndryl-Materialien oder Unternehmenssysteme). Die einzigen Services und Liefergegenstände des Lieferanten bestehen in der Bereitstellung von Vor-Ort-Software für Kyndryl oder der Lieferant erbringt alle seine Services und Liefergegenstände im Rahmen eines Personalverstärkungsmodells gemäß Artikel VII, einschließlich Abschnitt 1.7.

Der Lieferant erfüllt die Anforderungen dieses Artikels und schützt dadurch: (a) Kyndryl-Materialien gegen Verlust, Vernichtung, Veränderung, versehentliche oder unbefugte Weitergabe und zufälligen oder unbefugten Zugriff, (b) Kyndryl-Daten gegen rechtswidrige Formen der Verarbeitung und (c) die Kyndryl-Technologie gegen rechtswidrige Formen der Handhabung. Die Anforderungen dieses Artikels erstrecken sich auf alle IT-Anwendungen, -Plattformen und -Infrastrukturen, die der Lieferant bei der Erbringung von Lieferungen und Leistungen und bei der Handhabung der Technologie von Kyndryl betreibt oder verwaltet. Das schließt alle Entwicklungs-, Test-, Hosting-, Support-, Betriebs- und Rechenzentrumsumgebungen ein.

1. Sicherheitsrichtlinien

1.1 Der Lieferant befolgt und pflegt IT-Sicherheitsrichtlinien und -praktiken, die wesentliche Bestandteile des Geschäfts des Lieferanten sind, die für das gesamte Personal des Lieferanten obligatorisch sind und den Best Practices der Branche entsprechen.

1.2 Der Lieferant überprüft seine IT-Sicherheitsrichtlinien und -praktiken mindestens einmal jährlich und ergänzt sie, wenn der Lieferant es für notwendig erachtet, um die Kyndryl-Materialien zu schützen.

1.3 Der Lieferant wird die standardmäßigen, obligatorischen Anforderungen zur Überprüfung der Beschäftigung aller neu eingestellten Mitarbeiter pflegen und befolgen und diese Anforderungen auf das gesamte Personal des Lieferanten und die hundertprozentigen Tochtergesellschaften des Lieferanten ausweiten. Diese Voraussetzungen schließen Überprüfungen auf Vorstrafen ein, soweit dies nach lokalen Gesetzen zulässig ist und Überprüfung der Identitätsnachweise sowie zusätzliche Überprüfungen ein, die der Lieferant für erforderlich hält. Der Lieferant wiederholt diese Voraussetzungen regelmäßig und überprüft sie erneut, wenn er dies für erforderlich hält.

1.4 Der Lieferant schult seine Mitarbeiter jährlich in den Bereichen Sicherheit und Datenschutz und verlangt von allen diesen Mitarbeitern, jedes Jahr zu bestätigen, dass sie die ethischen Geschäftsleitlinien, Richtlinien zum Datenschutz und zur Sicherheit befolgen, wie dies in den Verhaltensregeln des Lieferanten oder ähnlichen Dokumenten festgelegt ist. Der Lieferant führt für Personen mit Verwaltungszugriff auf Komponenten der Services, Liefergegenstände oder Kyndryl-Materialien zusätzliche Richtlinen- und Verfahrensschulungen durch, die auf ihre Rolle und Unterstützung der Services, Liefergegenstände und Kyndryl-Materialien abgestimmt sind, und soweit erforderlich, um die erforderliche Konformität und Bescheinigungen zu gewährleisten.

1.5 Der Lieferant entwickelt Sicherheits- und Geheimhaltungsmaßnahmen, um die Verfügbarkeit von Kyndryl-Materialien zu schützen und zu pflegen, was auch ihre Implementierung, Pflege und Konformität mit Richtlinien und Verfahren einschließt, die schon aufgrund ihres Designs Sicherheit und Geheimhaltung, sichere Technik und sichere Operationen für alle Services und Liefergegenstände sowie und für die gesamte Handhabung der Technologie von Kyndryl erfordern.

2. Sicherheitsvorfälle

2.1 Der Lieferant pflegt und befolgt dokumentierte Incident-Response-Richtlinien, die Best Practices der Branche für die Vorfallshandhabung in der IT-Sicherheit entsprechen.

2.2 Der Lieferant untersucht unbefugte Zugriffe oder Nutzungen von Kyndryl-Materialien und definiert einen entsprechenden Interventionsplan und setzt diesen um.

2.3 Der Lieferant benachrichtigt Kyndryl unverzüglich (und keinesfalls später als 48 Stunden) nach Bekanntwerden einer Sicherheitsverletzung. Der Lieferant sendet eine solche Benachrichtigung an cyber.incidents@kyndryl.com. Der Lieferant wird Kyndryl in angemessener Weise Informationen über eine

solche Verletzung und den Status etwaiger Korrektur- und Wiederherstellungsmaßnahmen des Lieferanten zur Verfügung stellen. Zu den vernünftigerweise angeforderten Informationen können beispielsweise Protokolle gehören, die den privilegierten, administrativen und sonstigen Zugriff auf Geräte, Systeme oder Anwendungen nachweisen. Darüber hinaus können forensische Bilder von Geräten, Systemen oder Anwendungen und andere ähnliche Elemente angefordert werden, soweit sie für die Sicherheitsverletzung oder die Korrektur- und Wiederherstellungsmaßnahmen des Lieferanten relevant sind.

2.4 Der Lieferant unterstützt Kyndryl in angemessener Weise, um alle rechtlichen Verpflichtungen (einschließlich Meldeverpflichtungen gegenüber Aufsichtsbehörden oder betroffenen Personen) von Kyndryl, seinen verbundenen Unternehmen und Kunden (und deren Kunden und verbundenen Unternehmen) im Falle einer Sicherheitsverletzung zu erfüllen.

2.5 Der Lieferant wird Dritte nicht darüber informieren oder benachrichtigen, dass sich eine Sicherheitsverletzung direkt oder indirekt auf Kyndryl oder Kyndryl-Materialien bezieht, es sei denn, Kyndryl hat dies schriftlich genehmigt oder ist gesetzlich dazu verpflichtet. Der Lieferant benachrichtigt Kyndryl schriftlich vor der Herausgabe einer gesetzlich vorgeschriebenen Benachrichtigung an Dritte, wenn die Benachrichtigung die Identität von Kyndryl direkt oder indirekt offenlegen würde.

2.6 Im Fall einer Sicherheitsverletzung, die sich aus der Verletzung einer Verpflichtung im Rahmen dieser Bedingungen durch den Lieferanten ergibt:

(a) haftet der Lieferant für alle Kosten, die ihm entstehen, sowie für tatsächliche Kosten, die Kyndryl entstehen, wenn er zuständige Aufsichtsbehörden, andere Behörden und relevante branchenspezifische Selbstregulierungsbehörden, die Medien (falls nach geltendem Recht erforderlich), betroffene Personen, Kunden und andere über die Sicherheitsverletzung informiert.

(b) richtet der Lieferant auf Anfrage von Kyndryl auf eigene Kosten ein Call-Center ein und betreibt es, um Fragen von betroffenen Personen zu der Sicherheitsverletzung und ihren Folgen zu beantworten. Dies muss für die Dauer von einem (1) Jahr nach dem Datum vorgesehen sein, an dem die betroffenen Personen über die Sicherheitsverletzung informiert wurden, oder so lange, wie es das geltende Datenschutzrecht vorschreibt, je nachdem, was einen größeren Schutz bietet. Kyndryl und der Lieferant koordinieren, um die Skripte und andere Materialien zu erstellen, die von Call-Center-Mitarbeitern verwendet werden, wenn sie auf Rückfragen antworten. Alternativ kann Kyndryl auf schriftliche Mitteilung an den Lieferanten sein eigenes Call-Center einrichten und betreiben, anstatt den Lieferanten ein Call-Center einrichten zu lassen. In der Folge erstattet der Lieferant Kyndryl die tatsächlichen Kosten, die Kyndryl bei der Einrichtung und Verwaltung dieses Call-Centers entstehen, und

(c) der Lieferant wird Kyndryl die tatsächlichen Kosten erstatten, die Kyndryl durch die Bereitstellung von Kreditüberwachungs- und Kreditwiederherstellungsservices für ein (1) Jahr nach dem Datum entstehen, an dem von der Sicherheitsverletzung betroffene Personen, die sich dafür entscheiden, sich für solche Services einzutragen, über die Sicherheitsverletzung benachrichtigt wurden, oder nach Maßgabe der geltenden Datenschutzgesetze, je nachdem, was einen größeren Schutz bietet.

3. Physische Sicherheit und Zugangskontrolle (wie unten verwendet, bezeichnet „Einrichtung“ einen physischen Standort, an dem der Lieferant Kyndryl-Materialien hostet, verarbeitet oder anderweitig darauf zugreift).

3.1 Der Lieferant erhält geeignete physische Zugangskontrollen aufrecht, wie z. B. Schranken, Zugangspunkte mit Kartenkontrolle, Überwachungskameras und besetzte Empfangsschalter, um vor unbefugtem Zutritt zu Einrichtungen zu schützen.

3.2 Der Lieferant benötigt für den Zugang zu den Einrichtungen und kontrollierten Bereichen innerhalb der Einrichtungen, einschließlich des zeitlich begrenzten Zugangs, eine autorisierte Genehmigung und beschränkt den Zugang auf die jeweilige Funktion und den geschäftlichen Bedarf. Wenn der Lieferant vorübergehenden Zugang gewährt, wird sein bevollmächtigter Mitarbeiter jeden Besucher begleiten, während er sich in der Einrichtung und in den kontrollierten Bereichen aufhält.

3.3 Der Lieferant implementiert mechanische Zugangskontrollen, einschließlich Multi-Faktor-Zugangskontrollen, die den Best Practices der Branche entsprechen, um den Zugang zu kontrollierten Bereichen innerhalb der Einrichtungen in geeigneter Weise zu beschränken. Er wird alle Zugangsversuche protokollieren und diese Protokolle mindestens ein (1) Jahr aufheben.

3.4 Der Lieferant widerruft den Zugang zu Einrichtungen und kontrollierten Bereichen innerhalb von Einrichtungen, (a) bei Kündigung eines autorisierten Mitarbeiters des Lieferanten, oder (b) wenn für den autorisierten Mitarbeiter des Lieferanten keine gültige Geschäftsanforderung für den Zugang besteht. Der Lieferant hält formelle, dokumentierte Kündigungsverfahren ein, die eine unverzügliche Löschung aus Zugangskontrolllisten und die Aushändigung von Ausweisen für einen mechanischen Zugang einschließen.

3.5 Der Lieferant trifft Vorkehrungen, um die gesamte physische Infrastruktur, die zur Unterstützung der Services und Liefergegenstände und Handhabung der Technologie von Kyndryl verwendet wird, vor sowohl natürlich auftretenden als auch vom Menschen verursachten Umweltgefahren, wie übermäßige Umgebungstemperatur, Brände, Überschwemmungen, Feuchtigkeit, Diebstahl und Vandalismus zu schützen.

4. Zugriffs-, Interventions-, Übertragungs- und Trennungskontrolle

4.1 Der Lieferant hält die dokumentierte Sicherheitsarchitektur von Netzwerken aufrecht, die er in seinem Betrieb der Services, seiner Bereitstellung von Liefergegenständen und seiner Handhabung der Technologie von Kyndryl verwaltet. Der Lieferant wird diese Netzwerkarchitektur gesondert überprüfen und Maßnahmen ergreifen, um unbefugte Netzwerkverbindungen zu Systemen, Anwendungen und Netzwerkgeräten zu verhindern, und zwar im Hinblick auf die Einhaltung der Standards für sichere Segmentierung, Isolierung und tiefgreifende Verteidigung. Der Lieferant darf in seinem Hosting und Betrieb von gehosteten Services keine festnetzunabhängige Technologie einsetzen. Ansonsten darf der Lieferant bei seiner Bereitstellung von Services und Liefergegenständen und in seiner Handhabung der Technologie von Kyndryl festnetzunabhängige Technologie verwenden, wobei der Lieferant jedoch solche Drahtlosnetzwerke verschlüsseln und für sie eine sichere Authentifizierung verlangen muss.

4.2 Der Lieferant erhält Maßnahmen aufrecht, die dazu bestimmt sind, Kyndryl-Materialien logisch zu trennen und zu verhindern, dass sie von unbefugten Personen eingesehen oder ihnen zugänglich gemacht werden. Darüber hinaus pflegt der Lieferant eine angemessene Isolation seiner Produktions-, Nichtproduktions- und sonstigen Umgebungen. Soweit sich bereits Kyndryl-Materialien in einer nicht für die Produktion verwendeten Umgebung befinden oder in diese übertragen werden (z. B. um einen Fehler zu reproduzieren), stellt der Lieferant sicher, dass die Maßnahmen für Zugriffsschutz und Geheimhaltung in der nicht für die Produktion verwendeten Umgebung denen der Produktionsumgebung entsprechen.

4.3 Der Lieferant verschlüsselt Kyndryl-Materialien im Transit und im Ruhezustand (es sei denn, der Lieferant weist zur angemessenen Zufriedenheit von Kyndryl nach, dass die Verschlüsselung von Kyndryl-Materialien im Ruhezustand technisch nicht durchführbar ist). Der Lieferant verschlüsselt außerdem alle physischen Medien, falls vorhanden, wie z. B. Medien, die Sicherungsdateien enthalten. Der Lieferant pflegt in Verbindung mit Datenverschlüsselung dokumentierte Verfahren für eine sichere Erstellung, Ausstellung, Verteilung, Speicherung, Rotation, Aufhebung, Wiederherstellung, Sicherung, Vernichtung, und einen sicheren Zugriff auf und eine Verwendung von Schlüsseln. Der Lieferant stellt sicher, dass die für eine solche Verschlüsselung verwendeten spezifischen Verschlüsselungsverfahren den Best Practices der Branche (wie NIST SP SP 800-131a) entsprechen.

4.4 Wenn der Lieferant Zugriff auf Kyndryl-Materialien benötigt, beschränkt und begrenzt der Lieferant diesen Zugriff auf das niedrigste Niveau, das erforderlich ist, um die Services und Liefergegenstände bereitzustellen und zu unterstützen. Der Lieferant verlangt, dass ein solcher Zugriff, einschließlich des Verwaltungszugriffs auf alle zugrunde liegenden Komponenten (d. h. berechtigter Zugriff), individuell, rollenbasiert und vorbehaltlich der Genehmigung und regelmäßigen Überprüfung durch autorisierte Mitarbeiter des Lieferanten unter Einhaltung der Prinzipien zur Funktionstrennung erfolgt. Der Lieferant pflegt Maßnahmen, um überflüssige und ruhende Konten zu identifizieren und zu entfernen. Der Lieferant widerruft auch Konten mit berechtigtem Zugriff innerhalb von vierundzwanzig (24) Stunden nach der Kündigung des Kontoinhabers oder der Anfrage von Kyndryl oder eines autorisierten Mitarbeiters des Lieferanten, wie dem Manager des Kontoinhabers.

4.5 In Übereinstimmung mit Best Practices der Branche pflegt der Lieferant technische Maßnahmen zur Durchsetzung des Zeitlimits von inaktiven Sitzungen, für die Aussperrung von Konten nach mehreren, nacheinander fehlgeschlagenen Anmeldeversuchen, einer starken Kennwort- oder Kennphrasen-Authentifizierung sowie Maßnahmen, die eine sichere Übertragung und Speicherung solcher Passwörter und Kennphrasen erfordern. Darüber hinaus nutzt der Lieferant eine Multi-Faktor-Authentifizierung für alle nicht-konsolenbasierten privilegierten Zugriffe auf alle Kyndryl-Materialien.

4.6 Der Lieferant überwacht die Nutzung von berechtigtem Zugriff und pflegt Sicherheitsinformationen und Ereignismanagement-Maßnahmen mit dem Ziel: (a) unbefugte Zugriffe und Aktivitäten zu identifizieren, (b) eine rechtzeitige und angemessene Reaktion auf solche Zugriffe und Aktivitäten zu erleichtern, und (c) Überprüfungen durch den Lieferanten, Kyndryl (gemäß seinen Überprüfungsrechten in diesen Bedingungen und den Prüfungsrechten in dem Transaktionsdokument oder der zugehörigen Basis oder einer anderen damit verbundenen Vereinbarung zwischen den Parteien) und andere zu ermöglichen, um die Einhaltung der dokumentierten Richtlinien des Lieferanten zu überprüfen.

4.7 Der Lieferant bewahrt Protokolle auf, in denen er in Konformität mit Best Practices der Branche alle administrativen, Benutzer- oder sonstigen Zugriffe oder Aktivitäten auf oder in Bezug auf Systeme aufzeichnet, die bei der Bereitstellung von Services oder Liefergegenständen und Handhabung mit der Technologie von Kyndryl verwendet werden (und übermittelt Kyndryl diese Protokolle auf Anfrage). Der Lieferant trifft Maßnahmen zum Schutz vor unbefugten Zugriffen, Änderungen und der versehentlichen oder vorsätzlichen Vernichtung solcher Protokolle.

4.8 Der Lieferant pflegt Maßnahmen zum Schutz der Datenverarbeitung für Systeme, die er besitzt oder verwaltet, einschließlich Endbenutzersysteme, die er bei der Bereitstellung von Services oder Liefergegenständen oder Handhabung der Technologie von Kyndryl nutzt. Solche Schutzmaßnahmen sind u. a.: Endpunkt-Firewalls, vollständige Plattenverschlüsselung, signatur- und nicht-signaturbasierte Endpunkterkennung sowie Reaktionstechnologien zum Vorgehen gegen Malware und erweiterter persistenter Bedrohungen, zeitbasierten Bildschirmsperren und Endpunktmanagementlösungen, die Sicherheitskonfigurations- und Patching-Anforderungen umsetzen. Zusätzlich implementiert der Lieferant technische und operationale Kontrollinstrumente, die sicherstellen, dass nur bekannte und zuverlässige Endbenutzersysteme zur Nutzung von Lieferantennetzwerken zugelassen werden.

4.9 In Übereinstimmung mit Best Practices der Branche pflegt der Lieferant Schutzmaßnahmen für Rechenzentrumsumgebungen, in denen Kyndryl-Materialien vorhanden sind oder verarbeitet werden, wobei solche Schutzmaßnahmen die Erkennung von unbefugtem Zugriff und die Verhinderung sowie Gegenmaßnahmen und Risikominderung bei Denial-of Service-Angriffen einschließen.

5. Service- und Systemintegrität sowie Verfügbarkeitskontrolle

5.1 Der Lieferant: (a) führt mindestens jährlich Bewertungen zu Sicherheits- und Datenschutzrisiken durch, (b) führt Sicherheitstests durch und bewertet Schwachstellen, einschließlich automatisierter System- und Anwendungssicherheitsscans sowie manuelles Ethical Hacking vor dem Produktionsrelease und danach jährlich, soweit es sich um Services und Liefergegenstände handelt, und jährlich in Bezug auf seine Handhabung der Technologie von Kyndryl, (c) beteiligt einen qualifizierten unabhängig anderen Anbieter, um mindestens jährlich Penetrationstests nach den Best Practices der Branche durchzuführen, wobei diese Tests sowohl automatisierte als manuelle Test umfasst, (d) führt automatisierte Management- und Routineüberprüfungen der Konformität mit den Anforderungen der Sicherheitskonfiguration für jede Komponente der Services und Liefergegenständen und in Bezug auf seine Handhabung der Technologie von Kyndryl durch, und (e) korrigiert identifizierte Schwachstellen oder Nichtkonformitäten anhand der Anforderungen der Sicherheitskonfiguration basierend auf dem zugeordneten Risiko, der Exploit-Anfälligkeit und den Auswirkungen. Der Lieferant unternimmt angemessene Schritte, um eine Unterbrechung der Services zu vermeiden, wenn er seine Tests, Bewertungen, Scans und Korrekturmaßnahmen durchführt. Auf Anfrage von Kyndryl übermittelt der Lieferant Kyndryl eine schriftliche Zusammenfassung der jüngsten Penetrationstests des Lieferanten, die mindestens den Namen der von den Tests erfassten Angebote, die Anzahl der von den Tests erfassten Systeme oder Anwendungen, die Daten der Tests, die bei den Tests angewandte Methodik und eine Zusammenfassung der Ergebnisse auf höchster Ebene enthalten muss.

5.2 Der Lieferant pflegt Richtlinien und Verfahren im Hinblick auf das Management von Risiken, die mit der Umsetzung von Änderungen an den Services oder Liefergegenständen oder Handhabung der Technologie von Kyndryl verbunden sind. Vor der Implementierung einer solchen Änderung, auch an betroffenen Systemen, Netzwerken und zugrunde liegenden Komponenten, dokumentiert der Lieferant in einer registrierten Änderungsanforderung: (a) eine Beschreibung der Änderung und einen Grund für die Änderung, (b) die Implementierungsdetails und den Implementierungszeitplan, (c) eine Risikoaussage zu den Auswirkungen auf die Services und Liefergegenstände, Kunden der Services oder Kyndryl-Materialien, (d) das erwartete Ergebnis, (e) den Rollback-Plan und (f) die Genehmigung durch autorisierte Mitarbeiter des Lieferanten.

5.3 Der Lieferant führt einen Bestand aller IT-Assets, die er für den Betrieb der Services, für die Bereitstellung von Liefergegenständen und Handhabung der Technologie von Kyndryl verwendet. Der Lieferant überwacht und verwaltet kontinuierlich den Allgemeinzustand (einschließlich Nutzungsvolumen) und die Verfügbarkeit solcher IT-Assets, Services, Liefergegenstände und der zugrunde liegenden Technologie von Kyndryl, einschließlich der zugrunde liegenden Komponenten solcher Assets, Services, Liefergegenstände und Technologie von Kyndryl.

5.4 Der Lieferant wird alle Systeme, die er bei der Entwicklung oder dem Betrieb von Services und Liefergegenständen und der Handhabung der Technologie von Kyndryl verwendet, auf der Grundlage von vordefinierten Systemsicherheitsbildern oder Sicherheitsgrundlagen aufbauen, die den Best Practices der Branche entsprechen, wie z. B. den Benchmarks des Center for Internet Security (CIS).

5.5 Ohne Einschränkung der Verpflichtungen des Lieferanten oder der Rechte Kyndryls im Rahmen des Transaktionsdokuments oder der zugeordneten Basisvereinbarung zwischen den Parteien in Bezug auf unterbrechungsfreie Geschäftsabläufe, bewertet der Lieferant jeweils einzeln jeden Service, jeden Liefergegenstand und jedes IT-System, das bei der Handhabung mit der Technologie von Kyndryl verwendet wird, auf unterbrechungsfreie Geschäftsabläufe und IT-Kontinuität sowie Disaster-Recovery-Anforderungen gemäß den dokumentierten Richtlinien für das Risikomanagement. Der Lieferant stellt sicher, dass jeder dieser Services, Liefergegenstände und IT-Systeme, soweit durch eine solche Risikobeurteilung zugesichert, über separat definierte, dokumentierte, gepflegte und jährlich validierte Geschäfts- und IT-Kontinuitäts- und Disaster-Recovery-Pläne verfügt, die mit Best Practices der Branche in Einklang stehen. Der Lieferant stellt sicher, dass solche Pläne für die Erreichung der in Abschnitt 5.6 unten bestimmten Recovery-Zeiten konzipiert sind.

5.6 Die für den Recovery-Punkt („**RPO**“) und die Wiederherstellungszeit („**RTO**“) in Bezug auf einen gehosteten Service festgelegten Ziele betragen: 24 Stunden RPO und 24 Stunden RTO. Der Lieferant hält trotzdem jeden kürzeren Zeitraum für RPO oder RTO ein, die Kyndryl einem Kunden zugesagt hat, und dies unverzüglich nachdem Kyndryl den Lieferanten schriftlich über einen solchen kürzeren Zeitraum für den RPO oder die RTO informiert hat. (Eine E-Mail gilt als schriftliches Dokument.) Was alle anderen Services betrifft, die der Lieferant Kyndryl bereitstellt, muss der Lieferant sicherstellen, dass seine Pläne für unterbrechungsfreie Geschäftsabläufe und Disaster-Recovery so konzipiert sind, dass RPO und RTO erreicht werden, die es dem Lieferanten auch weiterhin ermöglichen, all seine Verpflichtungen gegenüber Kyndryl im Rahmen des Transaktionsdokuments und der zugeordneten Basisvereinbarung zwischen den Parteien und dieser Bedingungen, einschließlich seiner Verpflichtungen zur rechtzeitigen Erbringung von Test-, Support- und Wartungsleistungen, zu erfüllen.

5.7 Der Lieferant pflegt Maßnahmen, die dafür konzipiert sind, Security Advisory Patches für die Services und Liefergegenstände und zugeordnete Systeme, Netzwerke, Anwendungen und zugrunde liegende Komponenten innerhalb des Rahmens dieser Services und Liefergegenstände sowie für die Systeme, Netzwerke, Anwendungen, und zugrunde liegenden Komponenten zu bewerten, zu testen und umzusetzen, die für die Handhabung der Technologie von Kyndryl verwendet werden. Wenn festgestellt wird, dass ein Security Advisory Patch anwendbar und angemessen ist, implementiert der Lieferant den Patch gemäß den Richtlinien zum dokumentierten Schweregrad und zur Risikobeurteilung. Die Implementierung von Security Advisory Patches durch den Lieferanten wird in seiner Richtlinie für das Änderungsmanagement begründet.

5.8 Wenn Kyndryl Grund zu der Annahme hat, dass Hardware oder Software, die der Lieferant für Kyndryl bereitstellt, schädliche Elemente wie Spyware, Malware oder schädlichen Programmcode enthalten könnte, koordiniert der Lieferant zeitnah mit Kyndryl, um die Bedenken von Kyndryl zu untersuchen und zu beseitigen.

6. Servicebereitstellung

6.1 Der Lieferant unterstützt branchenspezifisch gängige Methoden der eingebundenen Authentifizierung für alle Benutzer oder Kundenkonten von Kyndryl, wobei der Lieferant bei der Authentifizierung solcher Benutzer von Kyndryl oder Kundenkonten von Kyndryl (wie z. B. von Kyndryl zentral verwaltetes Multi-Faktor-Single Sign-on über OpenID Connect oder Security Assertion Markup Language) die Best Practices der Branche anwendet.

7. Unterauftragnehmer Ohne Einschränkung der Verpflichtungen des Lieferanten oder der Rechte von Kyndryl gemäß dem Transaktionsdokument oder der zugeordneten Basisvereinbarung zwischen den Parteien in Bezug auf die Sicherung von Unterauftragnehmern, stellt der Lieferant sicher, dass jeder Unterauftragnehmer, der Aufträge für den Lieferanten durchführt, Governance-Kontrollinstrumente eingerichtet hat, um die Voraussetzungen und Verpflichtungen zu erfüllen, die dem Lieferanten durch diese Bedingungen auferlegt werden.

8. Physische Medien. Der Lieferant wird physische Medien, die für die Wiederverwendung bestimmt sind, vor der Wiederverwendung sicher desinfizieren und physische Medien, die nicht für die Wiederverwendung bestimmt sind, in Übereinstimmung mit den Best Practices der Branche für die Desinfektion von Medien vernichten.

Artikel IX, Zertifizierungen und Berichte der gehosteten Services

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

1.1 Der Lieferant holt die folgenden Zertifizierungen oder Berichte innerhalb des nachfolgend festgelegten Zeitrahmens ein:

Zertifizierungen / Berichte	**Zeitrahmen**
In Bezug auf die gehosteten Services des Lieferanten: Zertifizierung der Konformität mit ISO 27001, Informationstechnologie, Sicherheitstechniken, Managementsystemen für die Informationssicherheit, wobei eine solche Zertifizierung auf der Bewertung eines renommierten externen Prüfers basiert **oder** SOC 2 Typ 2: Ein Bericht eines renommierten externen Prüfers, der seine Überprüfung der Systeme, Kontrollinstrumente und Vorgänge des Lieferanten in Übereinstimmung mit einem SOC 2 Typ 2 nachweist (einschließlich, als Mindestanforderung, Sicherheit, Vertraulichkeit und Verfügbarkeit)	Der Lieferant erlangt die ISO 27001-Zertifizierung innerhalb von 120 Tagen nach dem Datum des Inkrafttretens des Transaktionsdokuments* oder des Annahmedatums** und erneuert die Zertifizierung danach alle 12 Monate auf der Grundlage der Bewertung eines renommierten unabhängigen Prüfers (wobei jede Erneuerung anhand der dann aktuellen Version der Norm erfolgt) Der Lieferant besorgt sich den SOC 2 Typ 2-Bericht innerhalb von 240 Tagen nach dem Datum des Inkrafttretens des Transaktionsdokuments* oder des Annahmedatums** und besorgt sich anschließend alle 12 Monate einen neuen Bericht eines renommierten unabhängigen Wirtschaftsprüfers, der die Überprüfung der Systeme, Kontrollen und Abläufe des Lieferanten gemäß SOC 2 Typ 2 (einschließlich mindestens Sicherheit, Vertraulichkeit und Verfügbarkeit) nachweist * Wenn der Lieferant ab Aktivierungsdatum einen gehosteten Service bereitstellt ** Das Datum, an dem der Lieferant eine Verpflichtung übernimmt, einen gehosteten Service bereitzustellen

1.2 Wenn der Lieferant schriftlich anfragt und Kyndryl dem schriftlich zustimmt, kann der Lieferant eine Zertifizierung oder einen Bericht anfordern, die den oben referenzierten im Wesentlichen gleich sind, wobei vorausgesetzt werden soll, dass die Zeitrahmen, die in der obigen Tabelle festgelegt wurden, in Bezug auf die wesentlich gleichen Zertifizierungen oder Berichte unverändert gelten sollen.

1.3 Der Lieferant: (a) übermittelt Kyndryl auf Anfrage unverzüglich eine Kopie jeder Zertifizierung und jedes Berichts, die der Lieferant einzuholen verpflichtet ist, und (b) behebt unverzüglich alle Schwachstellen interner Kontrollinstrumente, die während der SOC 2-Überprüfung oder wesentlich gleichen (falls Kyndryl dem zustimmt) festgestellt wurden.

Artikel X, Zusammenarbeit, Überprüfung und Korrektur

Dieser Artikel findet Anwendung, wenn der Lieferant Services oder Liefergegenstände für Kyndryl erbringt.

1. Lieferantenkooperation

1.1 Wenn Kyndryl Grund zu der Annahme hat, dass Services oder Liefergegenstände zu Bedenken hinsichtlich der Cybersicherheit beigetragen haben, beitragen oder beitragen werden, wird der Lieferant in angemessener Weise mit Kyndryl koordinieren. Das schließt die rechtzeitige und vollständige Beantwortung von Informationsanfragen ein, sei es durch Dokumente, andere Aufzeichnungen, Befragungen des zuständigen Personals des Lieferanten oder dergleichen.

1.2 Die Parteien verpflichten sich: (a) einander auf Anfrage weitere Informationen zu erteilen, (b) gegenseitig andere Dokumente zu unterzeichnen und zu übermitteln und (c) alle anderen Handlungen und Maßnahmen zu ergreifen, die die jeweils andere Partei vernünftigerweise verlangen kann, um die Absicht dieser Bedingungen und der in diesen Bedingungen genannten Dokumente zu erfüllen. Auf Anfrage von Kyndryl wird der Lieferant beispielsweise rechtzeitig die auf den Datenschutz und die Sicherheit ausgerichteten Bedingungen seiner schriftlichen Verträge mit Unterauftragsverarbeitern und Subunternehmern zur Verfügung stellen, einschließlich, sofern der Lieferant das Recht dazu hat, durch Gewährung von Zugang zu den Verträgen selbst.

1.3 Wenn Kyndryl dies verlangt, stellt der Lieferant Informationen über die Länder bereit, in denen seine Liefergegenstände und die Komponenten dieser Liefergegenstände hergestellt, entwickelt oder anderweitig abgeleitet wurden.

2. Überprüfung (wie unten verwendet, bezeichnet „Einrichtung“ einen physischen Standort, an dem der Lieferant Kyndryl-Materialien hostet, verarbeitet oder anderweitig darauf zugreift)

2.1 Der Lieferant pflegt einen protokollierbaren Datensatz, der die Einhaltung der Bedingungen belegt.

2.2 Kyndryl kann selbst oder mit Hilfe eines externen Prüfers nach schriftlicher Mitteilung an den Lieferanten 30 Tage im Voraus die Einhaltung dieser Bedingungen durch den Lieferanten überprüfen, auch durch den Zugang zu einer oder mehreren Einrichtungen zu diesem Zweck, wobei Kyndryl jedoch keinen Zugang zu einem Rechenzentrum erhält, in dem der Lieferant Kyndryl-Daten verarbeitet, es sei denn, er hat in gutem Glauben Grund zu der Annahme, dass dies zu relevanten Informationen führen könnte. Der Lieferant arbeitet bei der Überprüfung mit Kyndryl zusammen, was auch die rechtzeitige und vollständige Beantwortung von Informationsanfragen, sei es durch Dokumente, andere Aufzeichnungen, Interviews mit relevantem Personal des Lieferanten oder dergleichen, einschließt.Der Lieferant kann einen Nachweis über die Einhaltung genehmigter Verhaltensregeln oder eine branchenspezifische Zertifizierung vorlegen oder anderweitig Informationen bereitstellen, um Kyndryl die Einhaltung dieser Bedingungen zu belegen.

2.3 Eine Überprüfung findet nicht häufiger als einmal in einem 12-monatigen Zeitraum statt, es sei denn: (a) Kyndryl validiert die vom Lieferanten vorgenommene Behebung von Bedenken, bei einer früheren Überprüfung während des 12-monatigen Zeitraums auftraten, oder (b) es ist zu einer Sicherheitsverletzung gekommen und Kyndryl möchte die Einhaltung der für die Verletzung relevanten Verpflichtungen überprüfen. In beiden Fällen übermittelt Kyndryl 30 Tag vorab dieselbe schriftliche Mitteilung, wie in Abschnitt 2.2 oben angegeben, wobei jedoch die Dringlichkeit des Vorgehens gegen eine Sicherheitsverletzung es erfordern kann, dass Kyndryl eine Überprüfung innerhalb von weniger als 30 Tagen nach schriftlicher Mitteilung vornimmt.

2.4. Eine Aufsichtsbehörde oder ein anderer Verantwortlicher kann dieselben Rechte wie Kyndryl in den Abschnitten 2.2 und 2.3 ausüben, mit der Maßgabe, dass eine Aufsichtsbehörde weitere Rechte ausüben kann, die ihr nach dem Gesetz zustehen.

2.5 Wenn Kyndryl angemessenen Grund für die Schlussfolgerung hat, dass der Lieferant eine dieser Bedingungen nicht einhält (unabhängig davon, ob sich ein solcher Grund aus einer Überprüfung gemäß diesen Bedingungen oder anderweitig ergibt), behebt der Lieferant diese Nichteinhaltung unverzüglich.

3. Programm zur Bekämpfung von Produkt- und Markenpiraterie

3.1 Wenn die Liefergegenstände des Lieferanten elektronische Komponenten einschließen (z. B. Festplatten, Solid-State-Festplatten, Hauptspeicher, CPUs, Logikgeräte oder Kabel), pflegt und befolgt der Lieferant ein dokumentiertes Programm zur Fälschungsprävention, um in erster Linie zu verhindern, dass der Lieferant gefälschte Komponenten an Kyndryl liefert, und zweitens, unverzüglich jeden Fall erkennt und korrigiert, bei dem der Lieferant irrtümlicherweise gefälschte Komponenten an Kyndryl liefert. Der Lieferant verpflichtet in gleicher Weise alle seine Lieferanten, die elektronische Komponenten bereitstellen, die in den Liefergegenständen für Kyndryl eingeschlossen sind, ein dokumentiertes Programm zur Fälschungsprävention zu pflegen und zu befolgen.

4. Korrektur

4.1 Wenn der Lieferant eine seiner Verpflichtungen aus diesen Bedingungen nicht einhält und diese Unterlassung eine Sicherheitsverletzung verursacht, korrigiert der Lieferant seinen Leistungsausfall und behebt die schädlichen Auswirkungen der Sicherheitsverletzung, wobei diese Leistungserbringung und Korrektur nach der angemessenen Anweisung und dem Zeitplan von Kyndryl zu erfolgen haben. Wenn jedoch die Sicherheitsverletzung aus der Bereitstellung eines gehosteten Multi-Tenant-Service durch den Lieferanten entsteht und sich folglich auf zahlreiche Kunden des Lieferanten einschließlich Kyndryl auswirkt, dann korrigiert der Lieferant, je nach Spezifik der Sicherheitsverletzung, rechtzeitig und in angemessener Weise seinen Leistungsausfall und beseitigt die schädlichen Auswirkungen der Sicherheitsverletzung, wobei jeder Beitrag seitens Kyndryl zu solchen Korrekturen und Abhilfen gebührend berücksichtigt werden. Unbeschadet des oben Dargelegten muss der Lieferant Kyndryl unverzüglich benachrichtigen, wenn der Lieferant die durch das anwendbare Datenschutzrecht bestimmten Verpflichtungen nicht mehr einhalten kann.

4.2 Kyndryl hat das Recht, sich an der Korrektur einer Sicherheitsverletzung, auf die in Abschnitt 4.1 verwiesen wird, zu beteiligen, wie es dies für angemessen oder notwendig hält. Der Lieferant trägt seine Kosten und Ausgaben zur Korrektur seines Leistungsverhaltens und die Kosten und Ausgaben der Abhilfemaßnahmen, die den Parteien in Bezug auf eine solche Sicherheitsverletzung entstehen.

4.3 Zu den mit einer Sicherheitsverletzung verbundenen Abhilfekosten und -ausgaben könnten beispielsweise die Kosten für die Erkennung und Untersuchung einer Sicherheitsverletzung, die Bestimmung der Verantwortlichkeiten gemäß den geltenden Gesetzen und Vorschriften, die Bereitstellung von Benachrichtigungen über die Sicherheitsverletzung, die Einrichtung und Aufrechterhaltung von Call-Centern, die Bereitstellung von Kreditüberwachungs- und Kreditwiederherstellungsservices, das erneute Laden von Daten, die Korrektur von Produktfehlern (auch durch Quellcode oder andere Entwicklungen), die Beauftragung von Dritten zur Unterstützung bei den vorgenannten oder anderen relevanten Aktivitäten sowie andere Kosten und Ausgaben gehören, die zur Beseitigung der schädlichen Auswirkungen der Sicherheitsverletzung erforderlich sind. Zur Vermeidung von Missverständnissen: Kosten und Aufwendungen für Korrekturen würden für Kyndryl keine entgangenen Gewinne, Geschäfte, Wertverluste, Einnahmeausfälle, Verlust von Goodwill oder erwartete Einsparungen einschließen.