

## DATENSCHUTZ- UND SICHERHEITSBEDINGUNGEN FÜR LIEFERANTEN

Diese Datenschutz- und Sicherheitsbedingungen für Lieferanten legen die Rechte und Pflichten von Kyndryl sowie des Lieferanten in Bezug auf Datengovernance, Sicherheit und damit zusammenhängende Angelegenheiten fest (die „**Bedingungen**“). Die Bedingungen sind in die Lieferantenbeziehungsvereinbarung (oder eine gleichwertige Vereinbarung) zwischen den Parteien aufgenommen und Bestandteil davon, einschließlich Leistungsbeschreibungen, Arbeitsgenehmigungen oder anderer Dokumente, die zwischen den Unternehmen vereinbart wurden und auf sie verweisen („**Transaktionsdokumente**“).

Diese Bedingungen bestehen aus:

- diesem Dokument,
- der Verarbeitungsdetailsanlage die diesem Dokument beigelegt ist und in der die Datenverarbeitungsaktivitäten des Lieferanten zum Zeitpunkt der Unterzeichnung dieser Bedingungen dargelegt werden (für alle Transaktionsdokumente, die nach der Unterzeichnung dieser Bedingungen abgeschlossen werden, wird jedem Transaktionsdokument eine separate Verarbeitungsdetailsanlage beigelegt, in der die spezifischen Verarbeitungsaktivitäten des Lieferanten für dieses Dokument dokumentiert werden), und
- die EU-Standardvertragsklauseln, der Anhang zur internationalen Datenübertragung im Vereinigten Königreich sowie die Bewertung der Auswirkungen des Lieferantentransfers (Supplier Transfer Impact Assessment), die unter <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> zu finden sind.

Im Falle eines Widerspruchs zwischen diesen Bedingungen, der Lieferantenbeziehungsvereinbarung, einer gleichwertigen Vereinbarung oder einem Transaktionsdokument, einschließlich einer Datenverarbeitungsvereinbarung, haben diese Bedingungen Vorrang. Falls der Konflikt zwischen diesen Bedingungen und Bestimmungen besteht, die zwischen dem Lieferanten und Kyndryl für einen Kyndryl-Kunden vereinbart wurden, haben die für einen Kyndryl-Kunden vereinbarten Bestimmungen Vorrang.

Die in Großbuchstaben geschriebenen Begriffe haben die Bedeutungen, die in Artikel V dieser Bedingungen angegeben sind, es sei denn, sie werden in diesen Bedingungen, im Transaktionsdokument oder in der zugehörigen Basisvereinbarung zwischen den Parteien anders definiert.

### Article I. DATENGOVERNANCE UND KI

1.1. **Einhaltung von Gesetzen.** Der Lieferant hält alle Gesetze ein, die auf die Services und Liefergegenstände anwendbar sind, einschließlich der Gesetze über Datenschutz, Cybersicherheit und KI-Systeme. Der Lieferant benachrichtigt Kyndryl unverzüglich (und in jedem Fall innerhalb der gesetzlich vorgeschriebenen Fristen, die Kyndryl die Möglichkeit geben, seinen eigenen rechtlichen Verpflichtungen nachzukommen), wenn er feststellt, dass er seine rechtlichen Verpflichtungen nicht mehr erfüllen kann.

1.2. **Datennutzung.** Der Lieferant darf nicht:

- (a) Kyndryl-Daten in irgendeiner Form, einschließlich aggregierter, anonymisierter oder anderweitig verarbeiteter Daten, für andere Zwecke als die Erbringung der Services und Lieferung der Liefergegenstände verwenden. Beispielsweise darf der Lieferant Kyndryl-Daten nicht nutzen oder wiederverwenden, um die Wirksamkeit oder Verbesserungsmöglichkeiten seiner Angebote außerhalb der Services oder Liefergegenstände an Kyndryl zu bewerten, für Forschung und Entwicklung zur Erstellung neuer Angebote oder zur Erstellung von Berichten über seine Angebote.
- (b) Kyndryl-Daten verkaufen oder weitergeben oder
- (c) versuchen, Informationen zu reidentifizieren, die nach vernünftigem Ermessen verwendet werden können, um Rückschlüsse auf eine betroffene Person zu ziehen oder diese anderweitig zu identifizieren.

1.3. **Web-Tracking-Technologien.** Wenn der Lieferant oder seine Unterauftragnehmer bei der Erbringung der Services oder Lieferung der Liefergegenstände Daten mithilfe von Web-Tracking-Technologien (einschließlich HTML5, lokaler Speicherung, Tags oder Tokens von Dritten sowie Web-Beacons) erfasst, gelten diese Daten

als Kyndryl-Daten, und der Lieferant hält seine Verpflichtungen in Bezug auf Kyndryl-Daten gemäß diesen Bedingungen ein.

- 1.4. **Geheimhaltung.** Der Lieferant darf Kyndryl-Daten nicht an Dritte weitergeben, es sei denn, es handelt sich um Unterauftragsverarbeiter, die gemäß Abschnitt 2.5 genehmigt oder um Unterauftragnehmer, die gemäß der Vereinbarung zugelassen sind.
- 1.5. **Zugriff für Behörden.** Wenn eine Behörde, einschließlich einer Regulierungsbehörde, den Zugriff auf Kyndryl-Daten verlangt (z. B. wenn die US-Regierung dem Lieferanten einen nationalen Sicherheitsbefehl zur Beschaffung von Kyndryl-Daten zustellt) oder wenn eine Offenlegung von Kyndryl-Daten anderweitig gesetzlich vorgeschrieben ist, informiert der Lieferant Kyndryl unverzüglich schriftlich über ein solches Verlangen oder eine solche Anforderung und gibt Kyndryl eine angemessene Gelegenheit, einer Offenlegung zu widersprechen, sofern dies nicht gesetzlich verboten ist. Wenn die Benachrichtigung gesetzlich verboten ist, unternimmt der Lieferant die Schritte, die er nach vernünftigem Ermessen für angemessen hält, um das Verbot und die Offenlegung von Kyndryl-Daten durch gerichtliche Schritte oder andere Mittel anzufechten.
- 1.6. **Vertraulichkeit.** Der Lieferant sichert Kyndryl zu, dass: (a) nur diejenigen seiner Mitarbeiter Zugriff auf Kyndryl-Daten haben, die diesen Zugriff zur Erbringung von Services oder Lieferung von Liefergegenständen benötigen, und zwar nur in dem erforderlichen Umfang; und (b) er seine Mitarbeiter zur Vertraulichkeit verpflichtet hat, sodass diese Mitarbeiter Kyndryl-Daten nur in der Weise verwenden und offenlegen, wie es diese Bedingungen gestatten.
- 1.7. **Rückgabe oder Löschung von Kyndryl-Daten.** Der Lieferant löscht nach Wahl von Kyndryl die Kyndryl-Daten oder gibt sie Kyndryl auf eigene Kosten bei Beendigung oder Ablauf des Transaktionsdokuments oder auf Verlangen von Kyndryl früher zurück. Falls Kyndryl eine Löschung verlangt, macht der Lieferant gemäß NIST SP 800-88 Rev.1 die Daten unlesbar und verhindert, dass sie rekonstruiert oder wiederhergestellt werden können, und bestätigt die Löschung auf Anfrage von Kyndryl. Falls Kyndryl die Rückgabe von Kyndryl-Daten verlangt, gibt der Lieferant diese in einem gängigen Format und gemäß einem angemessenen Zeitplan sowie gemäß den Anweisungen von Kyndryl zurück.
- 1.8. **KI-Systeme**
  - (a) Der Lieferant darf ohne die vorherige Genehmigung von Kyndryl in einem Transaktionsdokument oder der Vereinbarung keine KI-Systeme bei der Erbringung der Services oder Lieferung eines Liefergegenstands verwenden oder KI-Systeme in einen Liefergegenstand einbeziehen. Der Lieferant stellt Kyndryl im Rahmen des Genehmigungsverfahrens schriftlich alle Informationen zur Verfügung, die zur Beurteilung des Einsatzes von KI-Systemen durch den Lieferanten erforderlich sind (z. B. Datenfluss, verwendete Sprachmodelle, Datentrennung).
  - (b) Der Lieferant sichert zu und gewährleistet, dass: (i) der von Kyndryl bereitgestellte Input (einschließlich des Inputs, der von den Mitarbeitern oder anderen Dritten im Rahmen eines Transaktionsdokuments bereitgestellt wird) und der Output als Kyndryl-Materialien eingestuft werden, (ii) der Lieferant die Kyndryl-Materialien nicht zum Training oder zur Feinabstimmung des Basismodells oder anderer Elemente der KI-Systeme verwendet, (iii) der Lieferant die Kyndryl-Materialien nicht länger aufbewahrt, als es für die Erbringung der Services erforderlich ist, (iv) die KI-Systeme (einschließlich der Outputs und der Trainingsdaten) als Teil der Services eingestuft werden und (v) der Lieferant hiermit, soweit dies nach geltendem Recht zulässig ist, alle seine Rechte, Titel und Interessen an den Outputs der KI-Systeme an Kyndryl abtritt.
  - (c) Der Lieferant muss ein dokumentiertes Governance- und Risikomanagementprogramm für die KI-Systeme einführen und aufrechterhalten, das bekannte und vorhersehbare Risiken identifiziert, prüft, überwacht und in angemessener Weise abmildert, einschließlich, aber nicht beschränkt auf Risiken in Bezug auf Ethik, Befangenheit, Sicherheit und Schutz, die mit den KI-Systemen verbunden sind oder sich daraus ergeben. Auf Anfrage stellt der Lieferant eine Kopie seines Governance- und Risikomanagementprogramms für KI-Systeme zur Verfügung. Der Lieferant informiert Kyndryl unverzüglich schriftlich über auftretende Risiken oder über ein identifiziertes erhebliches Risiko, gemäß der Mitteilungsklausel, die im Transaktionsdokument vereinbart wird, und sendet eine Kopie an [ailegalteam@kyndryl.com](mailto:ailegalteam@kyndryl.com).

## Article II. DATENSCHUTZ

- 2.1. **Geschäftskontaktinformationen.** Kyndryl und der Lieferant dürfen jeweils die Geschäftskontaktinformationen des anderen gemäß den geltenden Datenschutzgesetzen als unabhängige Verantwortliche verarbeiten, wo immer sie Geschäfte tätigen, um die Liefergegenstände und Services zu liefern bzw. zu erbringen und zu empfangen. Die Parteien handeln nicht als gemeinsame Verantwortliche in Bezug auf die Geschäftskontaktinformationen des jeweils anderen. Wenn eine der Parteien die andere über Anfragen eines Betroffenen in Bezug auf die Geschäftskontaktinformationen der anderen Partei informiert, ist die andere Partei dafür verantwortlich, solche Anfragen direkt mit dem Betroffenen zu besprechen. Jede der Parteien hat angemessene technische und organisatorische Maßnahmen ergriffen, um die Geschäftskontaktinformationen der anderen Partei zu schützen. Zur Klarstellung: Abschnitt 3.12 (Sicherheitsvorfälle) gilt ebenfalls für Geschäftskontaktinformationen.
- 2.2. **Der Lieferant als Auftragsverarbeiter.** Kyndryl ernennt den Lieferanten zum Auftragsverarbeiter seiner personenbezogenen Daten, und zwar ausschließlich zum Zweck der Bereitstellung der Liefergegenstände und Erbringung der Services gemäß den Anweisungen von Kyndryl, einschließlich der in diesen Bedingungen, der Vereinbarung und einem damit verbundenen Transaktionsdokument enthaltenen Anweisungen. Der Lieferant ist Auftragsverarbeiter von Kyndryls personenbezogenen Daten. Wenn der Lieferant nicht gemäß Kyndryls Anweisungen handelt, die für Kyndryl erforderlich sind, um die geltenden Datenschutzgesetze einzuhalten, kann Kyndryl den betroffenen Teil der Services durch schriftliche Mitteilung kündigen. Wenn der Lieferant der Ansicht ist, dass eine Anweisung gegen geltende Datenschutzgesetze verstößt, informiert er Kyndryl unverzüglich und innerhalb des gesetzlich vorgeschriebenen Zeitrahmens.
- 2.3. **Technische und organisatorische Maßnahmen.** Der Lieferant wird geeignete technische und organisatorische Maßnahmen, einschließlich der in Artikel III unten aufgeführten Sicherheitsmaßnahmen, implementieren und aufrechterhalten, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko im Zusammenhang mit der Erbringung der Services und Lieferung der Liefergegenstände angemessen ist.
- 2.4. **Rechte und Anfragen betroffener Personen**

- (a) Der Lieferant informiert Kyndryl unverzüglich (nach einem Zeitplan, der es Kyndryl und anderen Verantwortlichen ermöglicht, ihren gesetzlichen Verpflichtungen nachzukommen) über jede Anfrage einer betroffenen Person zur Ausübung von Betroffenenrechten (z. B. Berichtigung, Löschung oder Sperrung von Daten) in Bezug auf von Kyndryl verarbeitete personenbezogene Daten. Der Lieferant kann eine betroffene Person, die eine solche Anfrage stellt, auch unverzüglich an Kyndryl verweisen. Der Lieferant beantwortet keine Anfragen von betroffenen Personen, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Kyndryl schriftlich angewiesen.
- (b) Wenn Kyndryl verpflichtet ist, Informationen bezüglich der personenbezogenen Daten von Kyndryl an andere Verantwortliche oder andere Dritte (z. B. Betroffene oder Regulierungsbehörden) bereitzustellen, unterstützt der Lieferant Kyndryl, indem er Informationen bereitstellt und andere angemessene Maßnahmen ergreift, die Kyndryl anfordert, und zwar gemäß einem Zeitplan, der es Kyndryl ermöglicht, rechtzeitig auf solche anderen Verantwortlichen oder Dritte zu reagieren.

## 2.5. Unterauftragsverarbeiter

- (a) Kyndryl ermächtigt den Lieferanten, die in den jeweiligen Verarbeitungsdetailsanlagen aufgeführten Unterauftragsverarbeiter zu beauftragen. Kyndryl ermächtigt den Lieferanten ferner, zusätzliche oder ersetzende Unterauftragsverarbeiter zu beauftragen oder den Umfang der Verarbeitung durch einen bestehenden Unterauftragsverarbeiter zu erweitern, vorbehaltlich der folgenden Bedingungen:
  - (i) Der Lieferant informiert Kyndryl im Voraus schriftlich, bevor er einen neuen Unterauftragsverarbeiter hinzufügt oder einen bestehenden Unterauftragsverarbeiter ersetzt oder den Umfang der Verarbeitung durch einen bestehenden Unterauftragsverarbeiter erweitert.
  - (ii) Kyndryl kann jederzeit aus berechtigten Gründen gegen einen neuen oder ersetzten Unterauftragsverarbeiter oder eine Erweiterung des Umfangs Einspruch erheben. Erhebt Kyndryl einen solchen Einspruch, arbeiten die Parteien in gutem Glauben zusammen, um den Einspruch von Kyndryl zu klären.
  - (iii) Der Lieferant kann den neuen oder ersetzenden Unterauftragsverarbeiter beauftragen oder den Umfang der Verarbeitung des bestehenden Unterauftragsverarbeiters erweitern, wenn Kyndryl nicht innerhalb von 30 Tagen nach Erhalt der schriftlichen Mitteilung des Lieferanten Einspruch erhoben hat.
- (b) Der Lieferant verpflichtet jeden zugelassenen Unterauftragsverarbeiter zur Einhaltung der in diesen Bedingungen festgelegten Datenschutz-, Sicherheits- und Zertifizierungspflichten, bevor der Unterauftragsverarbeiter personenbezogene Daten von Kyndryl verarbeitet. Der Lieferant haftet Kyndryl gegenüber in vollem Umfang für die Erfüllung der Verpflichtungen jedes Unterauftragsverarbeiters.

## 2.6. Grenzüberschreitende Datenverarbeitung

- (a) Der Lieferant darf keine personenbezogenen Daten von Kyndryl grenzüberschreitend übertragen oder offenlegen (auch nicht durch Fernzugriff), es sei denn, sie werden gemäß Abschnitt 2.5 an zugelassene Unterauftragsverarbeiter weitergegeben. Wenn Kyndryl der grenzüberschreitenden Übertragung seiner personenbezogenen Daten zustimmt, arbeiten die Parteien zusammen, um die geltenden Datenschutzgesetze einzuhalten. Wenn diese Gesetze Standardvertragsklauseln (SCCs) erfordern, geht der Lieferant unverzüglich die unten definierten SCCs ein.
- (b) **Europäischer Wirtschaftsraum**
  - (i) Wenn Kyndryl personenbezogene Daten, die der DSGVO (2016/679) unterliegen, außerhalb des Europäischen Wirtschaftsraums an Lieferanten überträgt, die nicht in einem angemessenen Land ansässig sind, geht der Lieferant hiermit die EU-Standardvertragsklauseln (Beschluss 2021/914 der Kommission) ein, die von Kyndryl vorunterzeichnet wurden und unter <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> zu finden sind („EU-SCCs“).
  - (ii) Für den Fall, dass Kyndryl faktisch verschwinden, rechtlich nicht mehr existieren oder zahlungsunfähig werden sollte, haben die anderen für die Verarbeitung Verantwortlichen das Recht, die Vereinbarung zu beenden und den Lieferanten anzuweisen, die personenbezogenen Daten von Kyndryl zu löschen oder zurückzugeben.
  - (iii) Die von Kyndryl vorgenommene Bewertung der Übertragung personenbezogener Daten an Lieferanten, wie sie von den EU-SCCs gefordert wird, wird zur Einsichtnahme durch die Lieferanten unter <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> veröffentlicht.
  - (iv) Der Lieferant stellt ausreichende Details zu jedem Unterauftragsverarbeiter in den Verarbeitungsdetailsanlagen und Mitteilungen bereit, um seinen Verpflichtungen als Datenimporteur

- gemäß Klausel 14(c) der EU-Standardvertragsklauseln nachzukommen, einschließlich des Namens des Unterauftragsverarbeiters, der Verarbeitungsorte und der Verarbeitungstätigkeiten.
- (v) Der Lieferant fungiert als Datenexporteur und schließt mit jedem zugelassenen Unterauftragsverarbeiter, der nicht in einem angemessenen Land ansässig ist, EU-SCCs oder andere geeignete Übertragungsmechanismen ab.
  - (c) **Vereinigtes Königreich.** Wenn personenbezogene Daten von Kyndryl, die dem UK Data Protection Act (2018) unterliegen, außerhalb des Vereinigten Königreichs in ein nicht angemessenes Land übermittelt werden, geht der Lieferant hiermit dem von Kyndryl vorunterzeichneten Anhang zur internationalen Datenübertragung im Vereinigten Königreich ein, der sich unter [<https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>] befindet.
  - (d) **Schweiz.** Für den Fall, dass personenbezogene Daten von Kyndryl, die dem Schweizer Bundesgesetz über den Datenschutz („DSG“) unterliegen, ins Ausland in ein nicht angemessenes Land übertragen werden, geht der Lieferant hiermit vorbehaltlich der folgenden Änderungen die EU-SCCs ein:
    - (i) Verweise auf die DSGVO schließen auch den Verweis auf die entsprechenden Bestimmungen des DSG ein;
    - (ii) die Eidgenössische Datenschutzkommission ist die ausschließliche Aufsichtsbehörde gemäß Klausel 13 und Anhang I.C der EU-SCCs;
    - (iii) das maßgebende Recht gemäß Ziffer 17 der EU-SCCs ist das schweizerische Recht, sofern die Datenübertragung ausschließlich dem DSG untersteht; und
    - (iv) Der Begriff „Mitgliedstaat“ darf nicht so ausgelegt werden, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäß Artikel 18 der EU-SCCs einzuklagen.
  - (e) **Sonstige Länder.** Wenn die Übermittlung personenbezogener Kyndryl-Daten den Datenschutzgesetzen eines Landes unterliegt, in dem entweder die lokalen SCCs von der Aufsichtsbehörde nicht veröffentlicht wurden (z. B. brasilianisches Datenschutzgesetz, peruanisches Datenschutzgesetz, südafrikanisches Datenschutzgesetz) oder die Aufsichtsbehörde die Verwendung von EU-Standardvertragsklauseln als ausreichenden Schutz für die grenzüberschreitende Übermittlung genehmigt hat (z. B. argentinisches Datenschutzgesetz), gelten für eine solche Übermittlung die EU-SCCs vorbehaltlich der folgenden Änderungen:
    - (i) Verweise auf die DSGVO schließen auch den Verweis auf die entsprechenden Bestimmungen des örtlichen Datenschutzgesetzes ein;
    - (ii) die örtliche Aufsichtsbehörde ist die ausschließliche Aufsichtsbehörde gemäß Klausel 13 und Anhang I.C der EU-SCCs;
    - (iii) das geltende Recht gemäß Klausel 17 der EU-SCCs ist das örtliche Datenschutzrecht und
    - (iv) der Begriff „Mitgliedstaat“ darf nicht so ausgelegt werden, dass betroffene Personen in diesem Land von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort gemäß Paragraph 18 der EU-SCCs einzuklagen.

## 2.7. Unterstützung und Aufzeichnungen

- (a) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Lieferant Kyndryl durch geeignete technische und organisatorische Maßnahmen („TOMs“) bei der Erfüllung der Verpflichtungen im Zusammenhang mit Anfragen und Rechten der Betroffenen. Der Lieferant unterstützt Kyndryl auch dabei, die Einhaltung der Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Meldung und Kommunikation von Sicherheitsvorfällen sowie die Erstellung von Datenschutzfolgenabschätzungen sicherzustellen, einschließlich der vorherigen Konsultation mit der zuständigen Regulierungsbehörde, falls erforderlich, unter Berücksichtigung der dem Lieferanten verfügbaren Informationen.
- (b) Der Lieferant führt ein aktuelles Verzeichnis mit dem Namen und den Kontaktdaten jedes Unterauftragsverarbeiters, einschließlich des Vertreters und des Datenschutzbeauftragten des jeweiligen Unterauftragsverarbeiters. Der Lieferant stellt Kyndryl diese Aufzeichnungen auf Anfrage in einem Zeitrahmen zur Verfügung, der es Kyndryl ermöglicht, auf Anfragen von Kunden oder sonstigen Dritten rechtzeitig zu reagieren.

## 2.8. Länderspezifische Bedingungen

### (a) Japan

- i) Für Geschäftskontaktinformationen von betroffenen Personen, die in Japan ansässig sind, hält der Lieferant die Bedingungen ein, die für den Lieferanten als Auftragsverarbeiter gelten.

- ii) Die Definition des Begriffs „Sicherheitsvorfall“ in diesen Bedingungen wird hiermit geändert, um begründete Verdachtsfälle von Verletzungen der personenbezogenen Daten von Kyndryl in Bezug auf betroffene Personen in Japan einzuschließen.
  - iii) Der Lieferant garantiert, dass er keinen Grund zu der Annahme hat, dass die Gesetze und Praktiken eines Landes, in dem er oder seine Unterauftragsverarbeiter die personenbezogenen Daten von Kyndryl verarbeitet bzw. verarbeiten, den Lieferanten daran hindern, seine Verpflichtungen gemäß diesen Bedingungen zu erfüllen. Der Lieferant benachrichtigt Kyndryl, wenn er nach der Zustimmung zu den Bedingungen und während der Dauer der Bedingungen Grund zu der Annahme hat, dass er seinen Verpflichtungen aus den Bedingungen nicht nachkommen kann. In diesem Fall arbeiten die Parteien nach Treu und Glauben zusammen, um geeignete Maßnahmen zur Behebung der Situation zu finden. Wenn keine geeigneten Maßnahmen ergriffen werden können, prüft Kyndryl, ob die Übertragung personenbezogener Daten von Kyndryl ausgesetzt werden soll.
- (b) **Kalifornien.** Wo der Lieferant als Auftragsverarbeiter Kyndryl personenbezogene Daten von betroffenen Personen verarbeitet, die sich im Bundesstaat Kalifornien befinden, gilt Folgendes: (i) Kyndryl stellt dem Lieferanten die personenbezogenen Daten von Kyndryl ausschließlich für die in den jeweiligen Verarbeitungsdetailsanlage festgelegten, begrenzten und spezifischen geschäftlichen Zwecke zur Verfügung, (ii) Kyndryl kann, nach Benachrichtigung, angemessene und geeignete Maßnahmen ergreifen, um unbefugte Verarbeitung zu stoppen oder sicherzustellen, dass die Verarbeitung des Lieferanten mit den Verpflichtungen von Kyndryl unter den geltenden Datenschutzgesetzen übereinstimmt, und (iii) der Lieferant darf die personenbezogenen Daten von Kyndryl nicht außerhalb der direkten Geschäftsbeziehung zwischen Kyndryl und dem Lieferanten aufbewahren, verwenden oder weitergeben.

### Article III. ALLGEMEINE SICHERHEIT

#### 3.1. Sicherheitsrichtlinien

- (a) **Richtlinien.** Die Informationssicherheitsrichtlinien des Lieferanten werden dokumentiert, von der Geschäftsleitung des Lieferanten genehmigt und entsprechen den branchenüblichen Praktiken. Die Informationssicherheitsrichtlinien des Lieferanten werden vom Lieferanten mindestens einmal jährlich und unverzüglich nach wesentlichen Änderungen der Richtlinien überprüft und bewertet, damit festgestellt werden kann, ob sie weiterhin anwendbar und wirksam sind. Der Lieferant nimmt keine Änderungen an den Richtlinien vor, die die Sicherheit des Lieferanten in Bezug auf die Kyndryl-Materialien, die Liefergegenstände oder die Services beeinträchtigen würden.
- (b) **Testen.** Der Lieferant unterhält ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit seiner technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Kyndryl-Materialien, der Liefergegenstände und der Services.
- (c) **Risikomanagement.** Der Lieferant führt im Rahmen eines fortlaufenden Risikomanagementprogramms angemessene Informationssicherheitsrisikobewertungen durch, mit den folgenden Zielen: (i) Identifizierung von Informationssicherheitsrisiken im Zusammenhang mit den Kyndryl-Materialien, den Liefergegenständen und den Services; (ii) Bewertung der Auswirkungen solcher Risiken; und (iii) falls Risikominderungs- oder Abmilderungsstrategien identifiziert oder erforderlich sind, werden Maßnahmen ergriffen, um diese Risiken zu mindern und effektiv zu managen, wobei berücksichtigt wird, dass sich die Bedrohungslage ständig verändert.

#### 3.2. Personalsicherheit

- (a) **Sicherheitsschulung.** Der Lieferant stellt allen Mitarbeitenden, die Zugriff auf Kyndryl-Materialien, Liefergegenstände oder Services haben oder diesen Zugriff erlangen können, mindestens einmal jährlich entsprechende Sicherheits- und Datenschutzbewusstseinsbildung sowie entsprechende Schulungen bereit.
- (b) **Hintergrundüberprüfung.** Der Lieferant muss die standardmäßigen, obligatorischen Anforderungen zur Überprüfung des Beschäftigungsverhältnisses für alle neu eingestellten Mitarbeiter beibehalten und befolgen sowie diese Anforderungen auf das gesamte Personal des Lieferanten und das Personal der vom Lieferanten kontrollierten Tochtergesellschaften ausweiten. Zu diesen Anforderungen gehören die Überprüfung des strafrechtlichen Hintergrunds, soweit dies nach den örtlichen Gesetzen zulässig ist, die Überprüfung des Identitätsnachweises und zusätzliche Überprüfungen, die der Lieferant für erforderlich hält. Der Lieferant überprüft diese Anforderungen in regelmäßigen Abständen, wenn er dies für notwendig hält.

#### 3.3. Asset-Management

- (a) **Bestandserfassung.** Der Lieferant hält eine Bestandserfassung aller Geräte, auf denen Kyndryl-Materialien gespeichert sind, aufrecht. Der Lieferant gewährt nur autorisiertem Personal des Lieferanten Zugriff auf diese Geräte. Der Lieferant verhindert den unbefugten Zugriff auf und das Kopieren, Ändern oder Entfernen von Kyndryl-Materialien. Der Lieferant ergreift Maßnahmen zur Verhinderung des unbefugten Zugriffs, Kopierens, Ändern oder Löschens von Kyndryl-Materialien.
- (b) **Sicherheit von Softwarekomponenten.** Der Lieferant verpflichtet sich, alle Softwarekomponenten (einschließlich Open-Source-Software), die bei der Erbringung der Services sowie der Entwicklung und Bereitstellung der Liefergegenstände verwendet werden, in angemessener Weise zu inventarisieren. Der Lieferant prüft, ob solche Softwarekomponenten Sicherheitsmängel und/oder Schwachstellen aufweisen, die zu einer unbefugten Offenlegung von oder einem unbefugten Zugriff auf Kyndryl-Materialien, die Liefergegenstände oder Services führen könnten. Der Lieferant führt eine solche Bewertung vor der Bereitstellung der Services und Liefergegenstände oder bevor Kyndryl Zugriff darauf erhält durch und danach fortlaufend während der Laufzeit des Transaktionsdokuments. Der Lieferant verpflichtet sich, etwaige Sicherheitsmängel oder -lücken in einer solchen Softwarekomponente, von denen er Kenntnis erlangt, zeitnah zu beheben. Der Lieferant reagiert unverzüglich auf alle Anfragen von Kyndryl, die sich darauf beziehen, ob ein Sicherheitsmangel oder eine Schwachstelle in einer solchen Softwarekomponente dem Lieferanten bekannt ist und/oder vom Lieferanten behoben wurde.

**3.4. Zugriffssteuerungsrichtlinie.** Der Lieferant hält eine angemessene rollenbasierte Zugriffssteuerungsrichtlinie sowie geeignete technische Zugriffssteuerungsmaßnahmen entsprechend den branchenüblichen Standards ein, um den Zugriff auf Kyndryl-Materialien und Lieferantenassets, die zur Erbringung der Services verwendet werden, ausschließlich auf autorisiertes Lieferantenpersonal zu beschränken und diesen Zugriff auf das notwendige Minimum zu begrenzen, um die Dienstleistungen und Liefergegenstände bereitzustellen und zu unterstützen.

### 3.5. Genehmigung

- (a) Der Lieferant hält Verfahren zur Erstellung und Löschung von Benutzerkonten ein, um den Zugriff auf alle Kyndryl-Materialien sowie alle internen Anwendungen und Assets des Lieferanten, die bei der Erbringung der Services und Bereitstellung der Liefergegenstände verwendet werden, zu gewähren und unverzüglich (und in jedem Fall innerhalb von vierundzwanzig (24) Stunden) zu widerrufen. Der Lieferant weist eine geeignete Autorität zu, die die Erstellung und Deaktivierung von Benutzerkonten sowie die Erhöhung oder Reduzierung von Zugriffsrechten für bestehende Konten genehmigt. Dies gilt auch für den Fall der Beendigung eines Beschäftigungs-, Vertrags- oder sonstigen Arbeitsverhältnisses mit dem Lieferanten oder bei einer Rollenänderung, wenn die betroffene Person diese Zugriffsrechte nicht mehr benötigt.
- (b) Der Lieferant führt und aktualisiert Aufzeichnungen über das Personal des Lieferanten, das zum Zugriff auf Systeme und Anlagen berechtigt ist, auf denen Kyndryl-Materialien und Liefergegenstände gespeichert sind oder von denen aus darauf zugegriffen werden kann oder die zur Bereitstellung der Services verwendet werden, und überprüft diese Aufzeichnungen mindestens vierteljährlich. Administratives und technisches Hilfspersonal darf nur dann Zugriff auf solche Systeme, Kyndryl-Materialien und -Liefergegenstände haben, wenn dies erforderlich ist, und unter der Voraussetzung, dass dieses Personal die geltenden technischen und organisatorischen Maßnahmen des Lieferanten einhält.
- (c) Der Lieferant stellt sicher, dass Benutzerkonten, die Zugriff auf solche Systeme und Assets haben, einzigartig sind und durch Passwörter geschützt werden, und Benutzerkonten nicht gemeinsam genutzt werden.

### 3.6. Authentifizierung

- (a) Der Lieferant beobachtet wiederholte Zugriffsversuche auf Informationssysteme und -assets.
- (b) Der Lieferant wendet Passwortschutzverfahren an, die dem Branchenstandard entsprechen und darauf ausgelegt sind, die Vertraulichkeit und Integrität von Passwörtern zu wahren, die in jedweder Form erstellt, zugewiesen, verteilt und gespeichert werden. Der Lieferant erstellt ein starkes, zufällig generiertes, komplexes Passwort oder eine Kennphrase oder fordert den Benutzer auf, ein solches bzw. eine solche zu erstellen und zu verwenden. Alternativ können geeignete Optionen wie digitale Zertifikate, Karten/Hardware-Tokens oder Biometrie verwendet werden.
- (c) Der Lieferant verwendet eine mehrstufige Authentifizierung, auch für den administrativen Zugriff auf Domänen und Cloud-Portale. Die Multi-Faktor-Authentifizierung kann Techniken wie die Verwendung von kryptografischen Zertifikaten, Einmalpasswörtern (OTP) oder biometrischen Verfahren umfassen.

### 3.7. Kryptographie

- (a) **Richtlinie.** Der Lieferant führt kryptografische Richtlinien und Standards ein, die den Branchenstandards entsprechen, um Kyndryl-Materialien zu schützen, einschließlich, wo angemessen, Pseudonymisierung und Verschlüsselung.
- (b) **Verschlüsselung.** Der Lieferant verschlüsselt die Kyndryl-Materialien während des Transports und im Ruhezustand. Verschlüsselungsalgorithmen müssen eingesetzt werden, um die Daten auf Sicherheitsniveaus zu schützen, die den branchenüblichen Standards entsprechen (wie NIST SP 800-131a), und müssen branchenweit anerkannte Hash-Funktionen verwenden, die mindestens so schützend sind wie die Verschlüsselung mit dem 256-Bit Advanced Encryption Standard (AES 256) im Ruhezustand und TLS v1.2 bei der Übertragung. Der Lieferant hält Schlüsselmanagementrichtlinien und -praktiken ein, die den branchenüblichen Standards entsprechen und die Anforderungen, Sicherheit, Rotation und den Lebenszyklus von Verschlüsselungsschlüsseln definieren, einschließlich Erstellung, Verteilung, Widerruf, Archivierung und Vernichtung.

### 3.8. Physische und umgebungsspezifische Sicherheit

- (a) **Zugang zu Einrichtungen.** Der Lieferant beschränkt den Zugang zu den Einrichtungen auf sein autorisiertes Personal.
- (b) **Schutz vor Störungen.** Der Lieferant ergreift angemessene Maßnahmen, um Systeme und Assets vor Stromausfällen und anderen Störungen, die durch Ausfälle unterstützender Versorgungsleistungen verursacht werden, zu schützen.
- (c) **Sichere Entsorgung oder Wiederverwendung von Geräten.** Der Lieferant stellt sicher, dass alle Kyndryl-Materialien vor der Entsorgung oder Wiederverwendung von Geräten, die Speichermedien enthalten, sicher gelöscht oder überschrieben werden, indem er Verfahren anwendet, die den branchenüblichen Praktiken entsprechen.

### 3.9. Betriebssicherheit

- (a) **Betriebsrichtlinie.** Der Lieferant unterhält geeignete Betriebs- und Sicherheitsverfahren, die dem gesamten Personal, das sie benötigt, zur Verfügung gestellt werden.
- (b) **Schutz vor Malware.** Der Lieferant setzt Antivirus- und Endpunkt-Management-Lösungen ein, um Anti-Malware-Kontrollen zu gewährleisten, die die Systeme und Ressourcen vor schädlicher Software schützen, einschließlich schädlicher Software, die aus öffentlichen Netzwerken stammt.
- (c) **Konfigurationsmanagement.** Der Lieferant muss über Richtlinien verfügen, die die Installation von Software und Hilfsprogrammen durch das Personal regeln.
- (d) **Änderungsmanagement.** Der Lieferant pflegt und implementiert Verfahren, um sicherzustellen, dass nur genehmigte und sichere Versionen des Codes, der Konfigurationen, Systeme und Anwendungen in Produktionsumgebungen bereitgestellt werden.
- (e) **Logische Trennung.** Der Lieferant sorgt für eine angemessene Isolierung seiner Produktions-, Nicht-Produktions- und anderer Umgebungen, und wenn Kyndryl-Materialien bereits in einer Nicht-Produktionsumgebung vorhanden sind oder in eine solche übertragen werden (z. B. um einen Fehler zu reproduzieren), dann stellt der Lieferant sicher, dass die Sicherheits- und Datenschutzmaßnahmen in der Nicht-Produktionsumgebung denen in der Produktionsumgebung entsprechen.

### 3.10. Kommunikationssicherheit

- (a) **Informationsübertragung.** Der Lieferant beschränkt durch Verschlüsselung den Zugriff auf Kyndryl-Materialien, die auf Medien gespeichert sind und physisch außerhalb der Einrichtungen transportiert werden. Der Lieferant stellt sicher, dass es möglich ist, zu überprüfen und festzustellen, in welchem Umfang Kyndryl-Materialien über Kommunikationsgeräte übertragen oder bereitgestellt wurden oder bereitgestellt werden können.
- (b) **Sicherheit von Netzwerk-Services.** Der Lieferant stellt sicher, dass für alle Netzwerkservices und -komponenten Sicherheitskontrollen und -verfahren eingeführt werden, die den branchenüblichen Praktiken entsprechen, unabhängig davon, ob diese Services intern erbracht oder ausgelagert werden.
- (c) **Erkennung von unbefugtem Zugriff.** Der Lieferant setzt Systeme zur Erkennung oder Verhinderung von unbefugtem Zugriff sowie Maßnahmen zum Schutz vor und zur Abwehr von DoS-Angriffen (Denial-of-Service) für alle Systeme ein, die zur Bereitstellung der Services und Liefergegenstände verwendet werden. Dies schließt kontinuierliche Überwachung zur Erkennung und Reaktion auf Sicherheitsvorfälle ein, sobald

diese identifiziert werden, sowie die Aktualisierung der Signaturdatenbank, sobald neue Versionen zur kommerziellen Nutzung verfügbar sind.

- (d) **Firewalls.** Der Lieferant implementiert Firewalls, die nur dokumentierte und genehmigte Ports und Services zulassen. Alle anderen Ports werden im „Deny-All“-Modus (abgelehnt) betrieben.
- (e) **Überwachung.** Der Lieferant überwacht die Nutzung privilegierter Zugriffe und setzt Sicherheitsinformations- und Ereignismanagementmaßnahmen ein, um: (i) unbefugten Zugriff und Aktivitäten zu identifizieren, (ii) eine zeitnahe und angemessene Reaktion auf solchen Zugriff und solche Aktivitäten zu ermöglichen und (iii) Audits durch Kyndryl zu unterstützen.
- (f) **Protokollierung.** Der Lieferant muss Verfahren anwenden, die sicherstellen, dass alle Systeme, einschließlich Firewalls, Router, Netzwerk-Switches und Betriebssysteme, Informationen in ihren jeweiligen Systemprotokollen oder in einem zentralen Protokollierungssystem protokollieren, um die nachstehend erwähnten Sicherheitsaudits zu ermöglichen. Der Lieferant muss: (i) Protokolle mindestens 180 Tage lang aufbewahren, (ii) sicherstellen, dass keine Protokolle vertrauliche Informationen enthalten, (iii) Protokolle vor unbefugter Änderung oder Löschung schützen, (iv) täglich eine Sicherungskopie der Protokolle erstellen und (v) Protokolle auf Risiken und Funktionsanomalien überwachen. Der Lieferant stellt Kyndryl auf Anfrage solche Protokolle zur Verfügung.

### 3.11. Systembeschaffung, -entwicklung und -wartung

#### (a) Abschottung der Anwendung

- i) Der Lieferant verpflichtet sich, Richtlinien, Verfahren und Standards für die sichere Anwendungsentwicklung einzuhalten und zu implementieren. Diese müssen mit den branchenüblichen Praktiken übereinstimmen, wie z. B. den SANS Top 25 Security Development Techniques oder dem OWASP Top Ten-Projekt.
- ii) Das gesamte Personal des Lieferanten, das für den Entwurf, die Entwicklung, die Konfiguration, das Testen und den Einsatz sicherer Anwendungen verantwortlich ist, muss für die Erbringung der Services und Liefergegenstände qualifiziert sein und eine angemessene Schulung in Bezug auf die Praktiken des Lieferanten zur Entwicklung sicherer Anwendungen erhalten.

#### (b) Abschottung des Systems

- i) Der Lieferant stellt sicher, dass standardisierte, sichere Konfigurationen von Betriebssystemen verwendet werden. Images sollten abgeschottete Versionen des zugrunde liegenden Betriebssystems und der auf dem System installierten Anwendungen darstellen. Abschottung umfasst die Entfernung unnötiger Konten (einschließlich Servicekonten), das Deaktivieren oder Entfernen unnötiger Services, das Anwenden von Patches, das Schließen offener und ungenutzter Netzwerkports sowie die Implementierung von Einbruchserkennungs- und/oder Einbruchsverhinderungssystemen. Diese Images sollten regelmäßig validiert werden, um ihre Sicherheitskonfiguration bei Bedarf zu aktualisieren. Der Lieferant implementiert Patch-Tools und -Prozesse sowohl für Anwendungen als auch für Betriebssystem-Software. Wenn veraltete Systeme nicht mehr gepatcht werden können, aktualisiert der Lieferant die Anwendungssoftware auf die neueste Version. Der Lieferant entfernt veraltete, nicht unterstützte und ungenutzte Software vom System.
  - ii) Der Lieferant beschränkt Administratorrechte auf diejenigen Mitarbeiter, die sowohl über das notwendige Wissen zur Verwaltung des Betriebssystems verfügen als auch geschäftlich notwendig sind, um die Konfiguration des zugrunde liegenden Betriebssystems zu ändern.
- (c) **Scannen von Infrastrukturschwachstellen.** Der Lieferant scannt monatlich seine internen Umgebungen (z. B. Server, Netzwerktechnologien usw.), die mit den Services und Liefergegenständen verbunden sind, und wöchentlich die externen Umgebungen, die mit den Services und Liefergegenständen verbunden sind. Der Lieferant verfügt über einen festgelegten und dokumentierten Prozess mit spezifischen Zeitrahmen, um etwaige Vorkommnisse entsprechend dem bestehenden Risiko und dem Schweregrad zu beheben.
  - (d) **Bewertung der Anwendungsschwachstellen.** Der Lieferant führt vor jeder öffentlichen Veröffentlichung eine Analyse der Sicherheitslücken in der Anwendung durch. Der Lieferant verfügt über einen festgelegten und dokumentierten Prozess, um etwaige Vorkommnisse entsprechend dem bestehenden Risiko zu beheben.
  - (e) **Penetrationstests und Sicherheitsüberprüfungen.** Der Lieferant führt mindestens einmal jährlich einen umfassenden Penetrationstest und eine Sicherheitsüberprüfung aller Systeme durch, die an der Erbringung der Services und Bereitstellung der Liefergegenstände beteiligt sind. Darüber hinaus lässt der Lieferant eine jährliche Prüfung durch einen in der Branche anerkannten unabhängigen Dritten durchführen. Der Lieferant verfügt über einen festgelegten und dokumentierten Prozess, um etwaige Vorkommnisse entsprechend dem bestehenden Risiko zu beheben. Auf schriftliche Anfrage von Kyndryl, jedoch nicht mehr als einmal pro

Jahr, legt der Lieferant eine Bestätigung vor, aus der hervorgeht, dass ein unabhängiger Penetrationstest durchgeführt wurde und der Lieferant einen Prozess implementiert hat, um Feststellungen gemäß einer Risikobewertung zu beheben. Der Lieferant stellt eine Zusammenfassung der Ergebnisse zur Verfügung, einschließlich der Anzahl der getesteten Systeme oder Anwendungen, der Testdaten, der Testmethodik und der Anzahl der kritischen, schwerwiegenden, mittelschweren und geringfügigen Mängel.

- (f) **Notfallwiederherstellung.** Während der Laufzeit der Vereinbarung verfügt der Lieferant über eine Lösung zur Notfallwiederherstellung („DR“) oder Hochverfügbarkeit („HA“) sowie einen entsprechenden Plan, der für die Services und Liefergegenstände gilt und den branchenüblichen Standards entspricht. Der Lieferant testet die DR- oder HA-Lösung und den entsprechenden Plan mindestens einmal jährlich. Darüber hinaus gewährleisten die Lösung und der entsprechende Plan:
- i) dass die installierten Systeme, die zur Erbringung der Services und Bereitstellung der Liefergegenstände verwendet werden, im Falle einer Unterbrechung wiederhergestellt werden,
  - ii) die Fähigkeit des Lieferanten, die Verfügbarkeit und den Zugriff auf die Kyndryl-Materialien im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen, und
  - iii) die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der Systeme, die der Lieferant zur Erbringung der Services und Bereitstellung der Liefergegenstände nutzt.

### 3.12. Sicherheitsvorfälle

- (a) Der Lieferant unterhält und befolgt ein Programm zur Reaktion auf Datensicherheitsvorfälle, das den branchenüblichen Praktiken entspricht und dokumentierte Verfahren zur Untersuchung und Behandlung solcher Vorfälle umfasst. Das Programm zur Reaktion auf Vorfälle im Bereich der Datensicherheit befasst sich mit Themen wie der Priorisierung von Vorfällen, Rollen und Verantwortlichkeiten, internen Eskalationsverfahren, Nachverfolgung und Berichterstattung sowie Eindämmung und Behebung von Störungen. Das Programm für das Management von Sicherheitsvorfällen wird in regelmäßigen Abständen, mindestens jedoch jährlich, getestet, überprüft und genehmigt.
- (b) Der Lieferant informiert Kyndryl unverzüglich (und in keinem Fall später als 48 Stunden) nach Bekanntwerden eines Sicherheitsvorfalls per E-Mail an [cyber.incidents@kyndryl.com](mailto:cyber.incidents@kyndryl.com). In Bezug auf einen Sicherheitsvorfall ist der Lieferant verpflichtet, unverzüglich Folgendes zu tun:
- i) er muss Kyndryl in angemessener Weise Informationen über einen solchen Vorfall, über die Untersuchung des Vorfalls durch den Lieferanten und über den Status seiner Abhilfe- und Wiederherstellungsmaßnahmen zur Verfügung stellen; Beispielsweise können angemessenerweise angeforderte Informationen sachliche Feststellungen zur Art, Ursache und Auswirkung des Vorfalls umfassen, Protokolle, die den privilegierten, administrativen und sonstigen Zugang zu Geräten, Systemen, Services oder Anwendungen belegen, Zusammenfassungen auf der Grundlage von forensischen Bildern von Geräten, Systemen oder Anwendungen sowie andere ähnliche Elemente, soweit sie für den Vorfall oder die Abhilfe-, Behebungs- und Wiederherstellungsmaßnahmen des Lieferanten relevant sind;
  - ii) er muss dafür sorgen, dass die zuständigen Mitarbeiter des Lieferanten, die über den Vorfall informiert sind, an den von Kyndryl geforderten Telefonkonferenzen teilnehmen;
  - iii) er muss auf angemessene Anfrage von Kyndryl Drittanbieterexperten für Vorfalleaktion, Datenpannenmanagement, Forensik und elektronische Untersuchungen hinzuziehen;
  - iv) er muss Kyndryl angemessene Unterstützung leisten, damit Kyndryl, Kyndryl-Tochtergesellschaften und Kunden (sowie deren Kunden und Tochtergesellschaften) ihre rechtlichen Verpflichtungen (einschließlich der Verpflichtungen zur Benachrichtigung von Aufsichtsbehörden, betroffenen Personen, Kunden oder anderen Dritten) erfüllen können; und
  - v) er muss die Auswirkungen des Sicherheitsvorfalls zeitgerecht sowie angemessen mindern und beheben sowie zusätzliche Kontrollen und Prozesse implementieren, um das Risiko ähnlicher Vorfälle in der Zukunft zu verringern. Dabei muss er etwaige Rückmeldungen von Kyndryl zu solchen Minderungs- und Behebungsmaßnahmen angemessen berücksichtigen.
- (c) Der Lieferant ist für alle Kosten und Ausgaben verantwortlich, die ihm bei der Untersuchung, Reaktion, Abschwächung und Behebung eines Sicherheitsvorfalls entstehen. Vorbehaltlich der Haftungsbeschränkung in der Vereinbarung ist der Lieferant auch für alle Auslagen und Kosten verantwortlich, die Kyndryl, den mit Kyndryl verbundenen Unternehmen und Kunden (und deren Kunden und verbundenen Unternehmen) im Zusammenhang mit der Untersuchung, Reaktion, Milderung und Behebung des Sicherheitsvorfalls entstehen. Die Kosten und Ausgaben für die Behebung von Sicherheitsvorfällen können Kosten umfassen, die mit der Entdeckung und Untersuchung eines Sicherheitsvorfalls, der Festlegung von Verantwortlichkeiten

gemäß Gesetzen und Vorschriften, dem erneuten Laden von Daten, der Korrektur von Produktfehlern (einschließlich durch Quellcode oder andere Entwicklungen), der Beauftragung von Dritten zur Unterstützung bei den vorgenannten oder anderen relevanten Aktivitäten sowie anderen Kosten und Ausgaben, die zur Behebung der schädlichen Auswirkungen des Sicherheitsvorfalls erforderlich sind, zusammenhängen.

- (d) Im Falle eines Sicherheitsvorfalls, der personenbezogene Daten von Kyndryl betrifft, ist der Lieferant für alle anfallenden Kosten verantwortlich und erstattet Kyndryl alle Kosten und Ausgaben, die Kyndryl entstehen, und zwar:
- i) bei der Benachrichtigung der zuständigen Regulierungsbehörden, anderer staatlicher Stellen und einschlägiger Selbstregulierungsorganisationen der Branche, der Medien (sofern gesetzlich vorgeschrieben), der betroffenen Personen, der Kunden und anderer Personen über den Sicherheitsvorfall;
  - ii) bei der Einrichtung und Unterhaltung eines Call-Centers zur Beantwortung von Fragen betroffener Personen bezüglich des Sicherheitsvorfalls und seiner Folgen, und zwar für die Dauer eines Jahres nach dem Datum, an dem die betroffenen Personen über den Sicherheitsvorfall informiert wurden, oder länger, falls dies nach geltendem Datenschutzrecht erforderlich ist; bei der Zusammenarbeit von Kyndryl und dem Lieferanten bei der Erstellung und Bereitstellung von Skripten sowie anderen Materialien zur Verwendung durch das Call-Center-Personal bei der Beantwortung von Anfragen zu personenbezogenen Daten von Kyndryl; und
  - iii) bei der Bereitstellung von Services zum Schutz vor Identitätsdiebstahl, zur Kreditüberwachung und Kreditanierung für einen Zeitraum von zwei Jahren nach dem Datum, an dem die von dem Vorfall betroffenen Personen, die sich für solche Services registrieren lassen wollen, über den Sicherheitsvorfall benachrichtigt wurden, oder länger, falls dies nach geltendem Recht erforderlich ist.
- (e) Der Lieferant wird Kyndryl gegenüber Dritten weder direkt noch indirekt als von einem Sicherheitsvorfall betroffen identifizieren, es sei denn, Kyndryl erteilt dem seine schriftliche Zustimmung oder es ist gesetzlich vorgeschrieben. Der Lieferant informiert Kyndryl schriftlich, bevor er eine gesetzlich vorgeschriebene Mitteilung an einen Dritten weitergibt, die direkt oder indirekt die Identität von Kyndryl offenbart.
- (f) Der Lieferant informiert Kyndryl auch unverzüglich über jede tatsächliche oder drohende Verletzung dieser Bedingungen oder seiner Sicherheitsrichtlinien, Sicherheitsverfahren oder Richtlinien zur akzeptablen Nutzung im Zusammenhang mit der Lieferung eines Liefergegenstandes oder Erbringung der Services.

### **3.13. Lieferantenbeziehungen**

- (a) **Unterauftragnehmer.** Der Lieferant ist für die Einhaltung dieser Bedingungen verantwortlich, auch wenn er einen Unterauftragnehmer einsetzt. Der Lieferant verpflichtet die Unterauftragnehmer vertraglich, Kyndryl-Materialien durch Bedingungen zu schützen, die in keinem Fall weniger umfassend oder streng sind als die, die für den Lieferanten in den Vereinbarungsbedingungen gelten. Der Lieferant haftet gegenüber Kyndryl für die Erbringung der Leistungen eines jeden Unterauftragnehmers.
- (b) **Qualitätskontrolle und Sicherheitsmanagement.** Der Lieferant übernimmt die Qualitätskontrolle und die Überwachung des Sicherheitsmanagements der an einen Unterauftragnehmer ausgelagerten Softwareentwicklung.
- (c) **Vorvertragliche Informationen.** Der Lieferant versichert und garantiert, dass alle wesentlichen Informationen, die während der vorvertraglichen Gespräche mit Kyndryl in Bezug auf Datenschutz, Sicherheit und Datengovernance bereitgestellt wurden, sei es gemäß diesen Bedingungen oder anderweitig, wahrheitsgemäß und nicht, entweder durch Unterlassung oder auf andere Weise, irreführend sind.

### **3.14. Überprüfung, Zusammenarbeit, Sicherheitskonformität und Bewertung**

- (a) **Überprüfung** Der Lieferant führt ein prüfbares Protokoll, das die Einhaltung dieser Bedingungen nachweist.
- (i) Kyndryl kann selbst oder durch einen externen Prüfer 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 keinen Zugang zu einem Rechenzentrum erhält, in dem der Lieferant Kyndryl-Daten verarbeitet, es sei denn, Kyndryl hat in gutem Glauben Grund zu der Annahme, dass dies relevante Informationen liefern würde. Der Lieferant unterstützt die Überprüfung durch Kyndryl, indem er u. a. rechtzeitig und vollständig auf Auskunftersuchen antwortet, sei es durch Dokumente, sonstige Unterlagen, Befragungen des zuständigen Personals des Lieferanten oder dergleichen. Der Lieferant kann einen Nachweis über die

- Einhaltung eines genehmigten Verhaltenskodex oder einer Branchenzertifizierung vorlegen oder auf andere Weise Informationen bereitstellen, um die Einhaltung dieser Bedingungen Kyndryl gegenüber nachzuweisen.
- (ii) Eine Überprüfung findet nicht mehr als einmal innerhalb eines Zeitraums von zwölf Monaten statt, es sei denn: (A) Kyndryl validiert die Behebung von Problemen durch den Lieferanten, die sich aus einer früheren Überprüfung innerhalb des 12-Monats-Zeitraums ergeben haben, oder (B) es ist ein Sicherheitsvorfall aufgetreten und Kyndryl möchte die Einhaltung der für den Vorfall relevanten Verpflichtungen überprüfen. In jedem Fall informiert Kyndryl den Kunden dreißig Tage im Voraus schriftlich, wie in Absatz (i) oben beschrieben, aber die Dringlichkeit der Behebung eines Sicherheitsvorfalls kann es erforderlich machen, dass Kyndryl eine Überprüfung mit weniger als dreißig Tagen schriftlicher Vorankündigung durchführt.
  - (iii) Eine Regulierungsbehörde oder, soweit rechtlich zulässig, ein anderer für die Verarbeitung Verantwortlicher kann dieselben Rechte wie Kyndryl in den Absätzen (ii) und (iii) ausüben, wobei eine Regulierungsbehörde alle zusätzlichen Rechte ausüben kann, die ihr nach dem Gesetz zustehen.
  - (iv) Wenn Kyndryl einen angemessenen Grund zu der Annahme hat, dass der Lieferant eine dieser Bedingungen nicht erfüllt (unabhängig davon, ob dieser Grund aus einer Überprüfung gemäß diesen Bedingungen oder auf andere Weise entsteht), behebt der Lieferant diese Nicht-Einhaltung umgehend.
  - (v) Dieser Abschnitt gilt zusätzlich zu der Klausel „Aufzeichnungs- und Auditrecht“ oder einer anderen ähnlichen Auditklausel in der Vereinbarung.
- (b) **Zusammenarbeit.** Wenn Kyndryl Grund zu der Annahme hat, dass Services oder Liefergegenstände zu Bedenken im Bereich der Cybersicherheit beigetragen haben, beitragen oder beitragen werden, kooperiert der Lieferant in angemessener Weise bei allen Anfragen von Kyndryl zu solchen Problemen, einschließlich der rechtzeitigen und vollständigen Beantwortung von Informationsanfragen, sei es durch Dokumente, andere Aufzeichnungen, Befragungen des relevanten Personals des Lieferanten oder Ähnliches.
  - (c) **Sicherheitskonformität.** Der Lieferant erwirbt (i) eine Zertifizierung zur Einhaltung der ISO 27001 von einem unabhängigen Wirtschaftsprüfungsunternehmen, (ii) einen Bericht eines unabhängigen Wirtschaftsprüfungsunternehmens, der die Überprüfung der Systeme, Kontrollen und Betriebsabläufe des Lieferanten gemäß einem SOC 2 Typ 2 belegt, welcher mindestens die Trust Service Principles für Sicherheit (auch bekannt als die Gemeinsamen Kriterien), Verfügbarkeit und Vertraulichkeit umfasst, und (iii) einen Bericht eines unabhängigen Wirtschaftsprüfungsunternehmens, der die Überprüfung der Systeme, Kontrollen und Betriebsabläufe des Lieferanten gemäß einem SOC 1 Typ 2 belegt, falls die Services Auswirkungen auf die Finanzberichte von Kyndryl haben. Der Lieferant hält sich an künftige Richtlinien in Bezug auf SSAE18, die vom AICPA, IAASB, der Securities and Exchange Commission oder der Public Company Accounting herausgegeben werden. Der Lieferant stellt Kyndryl auf Anfrage unverzüglich eine Kopie aller Zertifikate und Berichte zur Verfügung, zu deren Beschaffung er verpflichtet ist.
  - (d) **Compliance-Bewertung durch Kyndryl.** Auf Kyndryls angemessene Anfrage, jedoch nicht mehr als einmal innerhalb eines Zeitraums von zwölf Monaten für jeden einzelnen Service oder Liefergegenstand, füllt der Lieferant einen Fragebogen genau und zeitnah (innerhalb von maximal 14 Tagen) aus, um Kyndryl bei der Überprüfung der Einhaltung der Verpflichtungen des Lieferanten in Bezug auf Cybersicherheit und Datengovernance gemäß der Vereinbarung und diesen Bedingungen zu unterstützen („**Compliance-Bewertung**“). Falls Kyndryl nach Abschluss der Compliance-Bewertung berechtigterweise feststellt, dass die Sicherheits- und Datengovernancepraktiken sowie -verfahren des Lieferanten nicht seinen Verpflichtungen entsprechen, benachrichtigt Kyndryl den Lieferanten über die Mängel. Falls der Lieferant der Bewertung von Kyndryl hinsichtlich der Mängel zustimmt, ist er verpflichtet, ohne unangemessene Verzögerung: (i) diese auf eigene Kosten innerhalb eines mit Kyndryl vereinbarten Zeitrahmens basierend auf einer Risikobewertung zu beheben und (ii) Kyndryl oder seinen ordnungsgemäß autorisierten Vertretern angemessene Dokumentation und Informationen zur Bestätigung der Behebung der Mängel bereitzustellen. Sollte der Lieferant als schwerwiegend oder kritisch eingestufte Mängel nicht innerhalb des vereinbarten Zeitrahmens beheben, hat Kyndryl das Recht, das betreffende Transaktionsdokument oder die Vereinbarung wegen erheblicher Verletzung sofort zu kündigen, nachdem der Lieferant darüber informiert wurde. Kyndryl darf die Unterlagen nur mit schriftlicher Zustimmung des Lieferanten an Dritte weitergeben, es sei denn, es handelt sich um eigene Auditoren. Wenn der Lieferant mit der Einschätzung von Kyndryl zu den Mängeln nicht einverstanden ist, übermittelt der Lieferant Kyndryl unverzüglich eine schriftliche Erklärung mit einer detaillierten Begründung, und falls Kyndryl die Gründe des Lieferanten nicht akzeptiert, leiten die Parteien die Angelegenheit zur umgehenden Klärung an ihren jeweiligen Datenschutzbeauftragten, Informationssicherheitsverantwortlichen oder eine vergleichbare Führungskraft mit ähnlichem

Verantwortungsbereich weiter. Sollten Mängel durch die Nutzung der Services durch Kyndryl verursacht werden, leistet der Lieferant angemessenen technischen Support, um Kyndryl bei der angemessenen Nutzung der Services zu unterstützen und die Mängel zu beheben.

#### **Article IV. ZUGRIFF AUF KYNDRYL-NETZWERKE**

Diese Bestimmung gilt, wenn Mitarbeiter des Lieferanten Zugriff auf ein Unternehmenssystem haben.

##### **4.1. Allgemeine Bedingungen**

- (a) Kyndryl entscheidet, ob die Mitarbeiter des Lieferanten Zugriff auf die Unternehmenssysteme erhalten sollen. Wenn Kyndryl dies genehmigt, hält der Lieferant die Anforderungen dieser Bestimmung ein und sorgt dafür, dass auch seine Mitarbeiter, die Zugriff haben, diese einhalten.
- (b) Kyndryl bestimmt die Mittel, mit denen die Mitarbeiter des Lieferanten auf die Unternehmenssysteme zugreifen können, einschließlich der Frage, ob diese Mitarbeiter über von Kyndryl oder vom Lieferanten bereitgestellte Geräte auf die Unternehmenssysteme zugreifen.
- (c) Die Mitarbeiter des Lieferanten dürfen nur zur Erbringung von Services auf die Unternehmenssysteme zugreifen und nur die Geräte verwenden, die von Kyndryl für diesen Zugriff autorisiert wurden, wobei es sich entweder um ein von Kyndryl bereitgestelltes Gerät („Kyndryl-Gerät“) oder ein vom Lieferanten bereitgestelltes Gerät („Lieferanten-Gerät“) handeln kann.
- (d) Die Mitarbeiter des Lieferanten dürfen Kyndryl-Materialien, die über ein Unternehmenssystem zugänglich sind, nur mit vorheriger schriftlicher Genehmigung von Kyndryl kopieren (und dürfen niemals Kyndryl-Materialien auf ein tragbares Speichermedium, wie z. B. einen USB-Stick, eine externe Festplatte oder ähnliche Geräte, übertragen).
- (e) Auf Anfrage bestätigt der Lieferant anhand der Namen seiner Mitarbeiter, auf welche Unternehmenssysteme diese im von Kyndryl angegebenen Zeitraum zugreifen dürfen bzw. zugegriffen haben.
- (f) Der Lieferant benachrichtigt Kyndryl innerhalb von vierundzwanzig (24) Stunden, wenn ein Mitarbeiter des Lieferanten, der Zugriff auf ein Unternehmenssystem hat, nicht mehr: (i) beim Lieferanten beschäftigt ist oder nicht mehr (ii) Tätigkeiten ausführt, die diesen Zugriff erfordern. Der Lieferant koordiniert mit Kyndryl, um sicherstellen, dass der Zugriff für solche ehemaligen oder aktuellen Mitarbeiter unverzüglich widerrufen wird.
- (g) Der Lieferant meldet Kyndryl unverzüglich alle tatsächlichen oder vermuteten Sicherheitsvorfälle (wie z.B. den Verlust eines Kyndryl- oder eines Lieferantengeräts oder den unbefugten Zugriff darauf oder auf Daten, Materialien oder andere Informationen jeglicher Art) und kooperiert mit Kyndryl bei der Untersuchung solcher Vorfälle.
- (h) Der Lieferant darf ohne die vorherige schriftliche Zustimmung von Kyndryl keinem Agenten, unabhängigen Auftragnehmer oder Mitarbeiter eines Unterauftragnehmers den Zugang zu einem Unternehmenssystem gestatten. Wenn Kyndryl diese Zustimmung erteilt, verpflichtet der Lieferant vertraglich diese Personen und deren Arbeitgeber, die Anforderungen dieses Artikels zu erfüllen, als ob diese Personen Mitarbeiter des Lieferanten wären, und ist Kyndryl gegenüber für alle Handlungen und Unterlassungen solcher Personen oder Arbeitgeber in Bezug auf den Zugang zu diesem Unternehmenssystem verantwortlich.
- (i) Kyndryl kann den Zugriff auf die Unternehmenssysteme jederzeit für einzelne oder alle Mitarbeiter des Lieferanten ohne vorherige Benachrichtigung sperren, wenn Kyndryl der Ansicht ist, dass dies zum Schutz von Kyndryl erforderlich ist.
- (j) Die Rechte von Kyndryl werden durch keine Bestimmung des Transaktionsdokuments, der zugehörigen Basisvereinbarung zwischen den Parteien oder einer anderen Vereinbarung zwischen den Parteien gesperrt, geschmälert oder in irgendeiner Weise eingeschränkt. Dies gilt auch für Bestimmungen, die vorschreiben, dass Daten, Materialien oder andere Informationen jeglicher Art nur an einem oder mehreren ausgewählten Orten aufbewahrt werden dürfen oder die vorschreiben, dass nur Personen von einem oder mehreren ausgewählten Orten auf diese Daten, Materialien oder anderen Informationen zugreifen dürfen.

##### **4.2. Gerätesoftware**

- (a) Der Lieferant weist sein Personal an, die notwendige Software, die Kyndryl zur sicheren Nutzung der Unternehmenssysteme benötigt, rechtzeitig auf Kyndryl- und Lieferantengeräten zu installieren. Weder der Lieferant noch dessen Personal beeinträchtigen die Funktionen der Software oder die Sicherheitsfunktionen, die von dieser aktiviert werden.

- (b) Der Lieferant und sein Personal halten sich an die von Kyndryl festgelegten Konfigurationsregeln für die Geräte von Kyndryl und die des Lieferanten und arbeiten auch sonst mit Kyndryl zusammen, um sicherzustellen, dass die Software wie von Kyndryl vorgesehen funktioniert. Beispielsweise setzt der Lieferant keine Funktionen der Software zum Blockieren von Websites oder Funktionen für automatisierte Patches außer Kraft.
- (c) Das Personal des Lieferanten darf Benutzernamen, Passwörter oder dergleichen für die Geräte von Kyndryl und die des Lieferanten nicht an andere Personen weitergeben.
- (d) Falls Kyndryl dem Personal des Lieferanten den Zugriff auf die Unternehmenssysteme über Lieferantengeräte erlaubt, installiert und führt der Lieferant ein Betriebssystem auf diesen Geräten aus, das von Kyndryl genehmigt wird, und aktualisiert es innerhalb eines angemessenen Zeitrahmens nach Anweisung von Kyndryl auf eine neue Version oder ein neues Betriebssystem.

#### 4.3. Kyndryl-Geräte

- (a) Mitarbeiter des Lieferanten dürfen die Kyndryl-Geräte nicht verwenden, um Services für andere Personen oder Unternehmen zu erbringen oder auf IT-Systeme, Netzwerke, Anwendungen, Websites, E-Mail-Tools, Kollaborationstools oder Ähnliches des Lieferanten oder Dritter zuzugreifen, die für oder im Zusammenhang mit den Services genutzt werden. Die Mitarbeiter des Lieferanten dürfen die Kyndryl-Geräte nicht für persönliche Zwecke verwenden (z. B. dürfen sie keine persönlichen Dateien wie Musik, Videos, Bilder oder andere ähnliche Elemente auf diesen Kyndryl-Geräten speichern und können das Internet von diesen Kyndryl-Geräten aus nicht für persönliche Zwecke nutzen). Die Mitarbeiter des Lieferanten dürfen die Kyndryl-Geräte, die sie zum Zugriff auf die Unternehmenssysteme verwenden, nicht mit anderen Mitarbeitern des Lieferanten teilen.
- (b) Kyndryl hat uneingeschränkte Rechte, die Kyndryl-Geräte und die Unternehmenssysteme zu überwachen und potenziellen unbefugten Zugriff sowie anderen Cybersicherheitsbedrohungen auf jede Art und Weise, von jedem Ort aus und mit allen Mitteln, die Kyndryl für notwendig oder angemessen hält, entgegenzuwirken, und zwar ohne vorherige Benachrichtigung des Lieferanten oder eines Mitarbeiters des Lieferanten oder anderer Personen. Als Beispiele für solche Rechte kann Kyndryl jederzeit (i) einen Sicherheitstest auf jedem Kyndryl-Gerät durchführen, (ii) Kommunikation (einschließlich E-Mails aus E-Mail-Konten auf den Kyndryl-Geräten), Aufzeichnungen, Dateien und andere Elemente, die auf einem Kyndryl-Gerät gespeichert oder über ein Unternehmenssystem übertragen werden, auf technische oder andere Weise überwachen, wiederherstellen und überprüfen und (iii) ein vollständiges forensisches Abbild eines Kyndryl-Geräts erstellen. Wenn Kyndryl zur Ausübung seiner Rechte die Mitwirkung des Lieferanten benötigt, kommt dieser den Anforderungen von Kyndryl in vollem Umfang und rechtzeitig nach (z. B. einschließlich der Anforderungen, ein Kyndryl-Gerät sicher zu konfigurieren, Überwachungs- oder andere Software auf einem Kyndryl-Gerät zu installieren, Verbindungsdetails auf Systemebene mitzuteilen, Maßnahmen zur Reaktion auf einen Vorfall auf einem Gerät zu ergreifen und physischen Zugriff auf ein Kyndryl-Gerät zu gewähren, damit Kyndryl ein vollständiges forensisches Abbild erhalten oder anderweitig darauf zugreifen kann, und ähnliche sowie damit in Zusammenhang stehende Anfragen).
- (c) Kyndryl behält das Eigentum an allen Kyndryl-Geräten, wobei der Lieferant das Risiko für den Verlust der Kyndryl-Geräte trägt, einschließlich durch Diebstahl, Vandalismus oder Fahrlässigkeit. Der Lieferant nimmt ohne vorherige schriftliche Zustimmung von Kyndryl keine Änderungen an Kyndryl-Geräten vor und gestattet auch keine derartigen Änderungen. Eine Änderung umfasst jede Veränderung an einem Gerät, einschließlich Änderungen an der Gerätesoftware, an Anwendungen, am Sicherheitsdesign, an der Sicherheitskonfiguration sowie am physischen, mechanischen oder elektrischen Design.
- (d) Der Lieferant gibt alle Geräte von Kyndryl innerhalb von fünf Werktagen zurück, nachdem die Geräte nicht mehr für die Erbringung von Services benötigt werden, und vernichtet auf Verlangen von Kyndryl gleichzeitig alle Daten, Materialien und sonstigen Informationen jeglicher Art auf diesen Geräten, ohne eine Kopie zurückzubehalten, indem er die NIST-Standards zur dauerhaften Löschung aller dieser Daten, Materialien und sonstigen Informationen befolgt. Der Lieferant verpackt die Kyndryl-Geräte und sendet sie auf eigene Kosten zurück. Sie müssen sich in demselben Zustand befinden, in dem sie geliefert wurden, abgesehen von normaler Abnutzung. Der Rückversand erfolgt an den von Kyndryl angegebenen Standort. Ein Verstoß des Lieferanten gegen eine Verpflichtung dieses Absatzes (d) stellt einen wesentlichen Verstoß gegen das Transaktionsdokument sowie die zugehörige Basisvereinbarung und alle damit in Verbindung stehenden Vereinbarungen zwischen den Parteien dar, wobei eine Vereinbarung als „in Verbindung stehend“ gilt, wenn der Zugriff auf ein Unternehmenssystem die Aufgaben oder sonstigen Tätigkeiten des Lieferanten im Rahmen dieser Vereinbarung erleichtert.

- (e) Kyndryl stellt Unterstützung für Kyndryl-Geräte bereit (einschließlich Geräteinspektion sowie präventiver und korrigierender Wartung). Der Lieferant informiert Kyndryl umgehend über den Bedarf an Korrekturmaßnahmen.
- (f) Für Softwareprogramme, die Kyndryl besitzt oder für die Kyndryl das Recht zur Lizenzierung hat, gewährt Kyndryl dem Lieferanten ein temporäres Recht zur Nutzung, Speicherung und zum Anfertigen ausreichender Kopien zur Unterstützung der autorisierten Nutzung von Kyndryl-Geräten. Der Lieferant ist nicht berechtigt, Programme an Dritte zu übertragen, Kopien von Softwarelizenzinformationen anzufertigen oder Programme zu disassemblieren, zu dekompileieren, rückzuentwickeln oder anderweitig zu übersetzen, es sei denn, dies ist nach geltendem Recht ohne die Möglichkeit eines vertraglichen Verzichts ausdrücklich zulässig.

## Article V. DEFINITIONEN

Die Begriffe „Services“ und „Liefergegenstände“ sind wahrscheinlich in der Lieferantenvereinbarung oder einer entsprechenden Vereinbarung oder einem Transaktionsdokument definiert; falls dies nicht der Fall ist, bedeutet „Services“ alle Hosting-, Beratungs-, Installations-, Anpassungs-, Wartungs-, Support-, Personalverstärkungs-, Geschäfts-, technischen oder anderen Arbeiten, die der Lieferant für Kyndryl gemäß dem Transaktionsdokument ausführt, und „Liefergegenstände“ bezeichnet alle Softwareprogramme, Plattformen, Anwendungen oder anderen Produkte oder Gegenstände sowie die zugehörigen Materialien, die der Lieferant gemäß dem Transaktionsdokument an Kyndryl liefert.

- 5.1. **Angemessenes Land** ist ein Land, das gemäß den geltenden Datenschutzgesetzen oder Entscheidungen der Regulierungsbehörden ein angemessenes Datenschutzniveau für die betreffende Übermittlung bietet.
- 5.2. **KI-System** bezeichnet ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren und nach der Bereitstellung anpassungsfähig sein kann, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, Rückschlüsse zieht, um Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen zu generieren, die physische oder virtuelle Umgebungen beeinflussen können.
- 5.3. **Geschäftskontaktinformationen** („BCI“) bezeichnet personenbezogene Daten, die verwendet werden, um eine Person in einer beruflichen oder geschäftlichen Funktion zu kontaktieren, zu identifizieren oder zu authentifizieren, und zwar für administrative und Vertragsmanagementzwecke (z. B. Rechnungsstellung und Kontoverwaltung, Berechnung von Partner-Incentives, interne Berichterstattung und Geschäftsmodellierung wie Prognosen, Umsatz- und Kapazitätsplanung). In der Regel enthalten Geschäftskontaktinformationen den Namen einer Person, ihre geschäftliche E-Mail-Adresse, ihre Anschrift, ihre Telefonnummer oder ähnliche Merkmale. Zum Beispiel sind Namen und E-Mail-Adressen, die verwendet werden, um Lieferantenpersonal für Support-Dienste zu kontaktieren, Geschäftskontaktinformationen. Jedoch stellen Namen und E-Mail-Adressen, die in diagnostischen Support-Daten enthalten sind, personenbezogene Daten von Kyndryl dar.
- 5.4. **Cloud-Service** bezeichnet jedes „As-a-Service“-Angebot, das der Anbieter hostet oder verwaltet, einschließlich „Software-as-a-Service“- „Platform-as-a-Service“- und „Infrastructure-as-a-Service“-Angebote.
- 5.5. **Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
- 5.6. **Unternehmenssystem** bezeichnet ein IT-System, eine Plattform, Anwendung, Netzwerk oder Ähnliches, auf das Kyndryl für seine Geschäftstätigkeit angewiesen ist, einschließlich der Systeme, die über Kyndryls Intranet, das Internet oder auf andere Weise zugänglich sind.
- 5.7. **Kunde** bezeichnet einen Kunden von Kyndryl.
- 5.8. **Datenimporteur** ist entweder ein Auftragsverarbeiter oder ein Unterauftragsverarbeiter, der nicht in einem angemessenen Land ansässig ist.
- 5.9. **Betroffener** bedeutet eine natürliche Person, die direkt oder indirekt identifiziert werden kann.
- 5.10. **Tag** oder **Tage** bezeichnet Kalendertage, es sei denn, es sind „Werktage“ angegeben.
- 5.11. **Gerät** bezeichnet eine von Kyndryl bereitgestellte oder vom Lieferanten bereitgestellte Workstation, einen Laptop, ein Tablet, ein Smartphone oder einen persönlichen digitalen Assistenten.
- 5.12. **Einrichtungen** bedeutet ein physischer Standort, an dem der Lieferant Liefergegenstände oder Kyndryl-Materialien hostet, darauf zugreift oder anderweitig verarbeitet.
- 5.13. **Branchenübliche Praktiken** bedeutet die von dem National Institute of Standards and Technology („NIST“) oder der International Organization for Standardization („ISO“) oder von anderen ähnlich renommierten und kompetenten Organisationen empfohlenen oder geforderten Praktiken.

- 5.14. **Kyndryl-Daten** sind alle Daten, Dateien, Materialien, Texte, Audio-, Video-, Bild- oder andere Daten, einschließlich personenbezogener Daten von Kyndryl, Geschäftskontaktinformationen von Kyndryl und nicht personenbezogener Daten von Kyndryl, die dem Lieferanten (insbesondere über einen Cloud-Dienst) im Zusammenhang mit der Erbringung der Services oder Lieferung eines Liefergegenstandes zur Verfügung gestellt oder zugänglich gemacht werden, unabhängig davon, ob sie von Kyndryl, Kyndryl-Personal, einem Kunden, einem Mitarbeiter oder Auftragnehmer des Kunden oder einer anderen natürlichen oder juristischen Person zur Verfügung gestellt oder zugänglich gemacht werden.
- 5.15. **Kyndryl-Materialien** sind alle Kyndryl-Daten und Kyndryl-Technologie.
- 5.16. **Persönliche Daten von Kyndryl** sind die personenbezogenen Daten, mit Ausnahme der Geschäftskontaktinformationen von Kyndryl, die Kyndryl dem Lieferanten für die Erbringung der Services oder Lieferung der Liefergegenstände zur Verfügung stellt oder zugänglich macht. Zu den personenbezogenen Daten von Kyndryl gehören personenbezogene Daten, die Kyndryl kontrolliert, sowie personenbezogene Daten, die Kyndryl im Auftrag anderer Verantwortlicher verarbeitet.
- 5.17. **Kyndryl-Technologie** bedeutet Quellcode, sonstiger Code, Beschreibungssprachen, Firmware, Software, Tools, Entwürfe, Schemata, grafische Darstellungen, eingebettete Schlüssel, Zertifikate und sonstige Informationen, Materialien, Assets, Dokumente und Technologie, die Kyndryl dem Lieferanten in Verbindung mit einem Transaktionsdokument oder der Vereinbarung direkt oder indirekt lizenziert oder anderweitig zur Verfügung gestellt hat.
- 5.18. **Nicht angemessenes Land** bezeichnet ein Land, das gemäß den geltenden Datenschutzgesetzen oder einer Entscheidung einer zuständigen Regulierungsbehörde nicht als angemessen gilt.
- 5.19. **Anderer Verantwortlicher** bezeichnet jedes andere Unternehmen als Kyndryl, das für Kyndryl-Daten verantwortlich ist, wie z. B. eine Tochtergesellschaft von Kyndryl, ein Kunde oder ein verbundenes Unternehmen eines Kunden.
- 5.20. **On-Premise-Software** bezeichnet Software, die vom Lieferanten als Liefergegenstand bereitgestellt wird und die von Kyndryl oder einem Kyndryl-Unterauftragnehmer auf den Servern oder Systemen von Kyndryl oder des Unterauftragnehmers ausgeführt, installiert oder betrieben wird.
- 5.21. **Personenbezogene Daten** bezeichnet alle Informationen, die sich auf eine betroffene Person beziehen, sowie alle anderen Informationen, die unter geltendem Datenschutzrecht als „personenbezogene Daten“ oder vergleichbare Daten eingestuft werden.
- 5.22. **Personal** bezeichnet folgende Personen: Angestellte von Kyndryl oder dem Lieferanten, Vertreter von Kyndryl oder dem Lieferanten, selbstständige Auftragnehmer, die von Kyndryl oder dem Lieferanten beauftragt wurden, oder Personen, die einer Partei von einem Unterauftragnehmer zur Verfügung gestellt werden.
- 5.23. **Verarbeitung** ist jeder Vorgang oder jede Reihe von Vorgängen, der/die mit Kyndryl-Daten durchgeführt wird/werden, einschließlich Speicherung, Verwendung, Zugriff und Lesen.
- 5.24. **Verarbeiter** ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, und umfasst auch „Service Provider“ oder vergleichbarer Begriffe, wie sie unter den geltenden Datenschutzgesetzen verwendet werden.
- 5.25. **Sicherheitsvorfall** bedeutet: (a) ein Ereignis, das tatsächlich oder unmittelbar die Vertraulichkeit, Integrität oder Verfügbarkeit von Kyndryl-Materialien oder einem Informationssystem gefährdet, das vom Lieferanten oder seinen Unterauftragnehmer zur Bereitstellung der Services oder Bereitstellung der Liefergegenstände verwendet wird, (b) ein Sicherheitsverstoß, der zur versehentlichen oder rechtswidrigen Zerstörung, Verlust, Veränderung, unbefugten Offenlegung oder zum unbefugten Zugriff auf Kyndryl-Daten führt, die übertragen, gespeichert oder anderweitig verarbeitet werden, oder (c) der unbefugte Zugriff auf oder die unbefugte Nutzung von Quellcode, der vom Lieferanten oder seinen Unterauftragnehmern bei der Bereitstellung der Services oder eines Liefergegenstands verwendet wird.
- 5.26. **Verkaufen** (oder **Verkauf**) bedeutet die Vermietung, Freigabe, Offenlegung, Verbreitung, Zurverfügungstellung, Übertragung oder anderweitige mündliche, schriftliche, elektronische oder sonstige Übertragung von Daten gegen Entgelt oder eine andere wertvolle Gegenleistung.
- 5.27. **Weitergeben** hat die Bedeutung, die im California Consumer Privacy Act von 2018, geändert durch das Consumer Privacy Rights Act von 2020, festgelegt ist.
- 5.28. **Standardvertragsklauseln** („SCCs“) bezeichnet die vertraglichen Klauseln, die gemäß den geltenden Datenschutzgesetzen für die Übertragung von personenbezogenen Daten an Verantwortliche oder Auftragsverarbeiter erforderlich sind, die nicht in einem angemessenen Land ansässig sind.
- 5.29. **Quellcode** bezeichnet einen von Menschen lesbaren Programmiercode oder einen Code, der in eine von Menschen lesbare Form umgewandelt werden kann und der von Entwicklern bei der Erstellung, Entwicklung

oder Wartung eines Produkts verwendet wird, aber im normalen Verlauf der kommerziellen Verbreitung oder Nutzung des Produkts nicht veröffentlicht wird.

- 5.30. **Unterauftragsverarbeiter** bezeichnet jeden Unterauftragnehmer des Lieferanten, einschließlich einer seiner Tochtergesellschaften, der die personenbezogenen Daten von Kyndryl verarbeitet.
- 5.31. **Aufsichtsbehörde** bezeichnet eine unabhängige staatliche Stelle, die für die Überwachung der Anwendung von Datenschutzgesetzen in einem bestimmten Land oder einer Region verantwortlich ist.