Kyndryl Datensicherheits- und Datenschutzrichtlinien

kyndryl

1. Begriffsbestimmungen

Begriffe, die in diesem Dokument verwendet werden, haben die nachstehend festgelegte Bedeutung. Begriffe, die nachstehend nicht definiert werden, haben die im zutreffenden schriftlichen Vertrag zwischen Kyndryl und dem Kunden über die Kyndryl Services festgelegte Bedeutung.

Kunde – bezeichnet das Unternehmen, für das Kyndryl die Kyndryl Services im Rahmen eines Kyndryl Servicedokuments bereitstellt.

Komponenten – bezeichnet die Anwendungs-, Plattform- oder Infrastrukturelemente eines Kyndryl Service, die Kyndryl betreibt und verwaltet.

Inhalte – bezeichnet sämtliche Daten, Software und Informationen, die vom Kunden oder seinen berechtigten Benutzern in Kyndryl Services bereitgestellt, für den Zugriff freigegeben oder eingegeben werden.

DSP – bezeichnet diese Kyndryl Datensicherheits- und Datenschutzrichtlinien (Data Security and Privacy Principles).

Kyndryl Servicedokument – bezeichnet ein Auftragsdokument oder ein beliebiges anderes Dokument, das in einen schriftlichen Vertrag zwischen Kyndryl und einem Kunden aufgenommen wird und Einzelheiten eines bestimmten Kyndryl Service enthält.

Kyndryl Services – bezeichnet (a) Kyndryl Serviceangebote, einschließlich Infrastruktur- oder Anwendungsserviceangeboten, die Kyndryl bereitstellt und für einen Kunden dediziert erbringt oder anpasst, und b) sonstige Services, wie z. B. Beratung, Wartung oder Unterstützung, die Kyndryl einem Kunden bereitstellt.

Sicherheitsvorfall – bezeichnet den unbefugten Zugriff auf Inhalte und deren unbefugte Verwendung.

Auftragsdokument – bezeichnet ein Dokument, das detaillierte Spezifikationen von Transaktionen enthält, wie z. B. Gebühren und eine Beschreibung eines Kyndryl Service sowie Informationen darüber. Beispiele für Auftragsdokumente sind unter anderem Leistungsbeschreibungen, Servicebeschreibungen, Bestellungen und Rechnungen für einen Kyndryl Service. Es kann mehr als ein Auftragsdokument für eine Transaktion geben.

2. Übersicht

Die in diesen DSP enthaltenen technischen und organisatorischen Maßnahmen gelten für Kyndryl Services (einschließlich Komponenten), sofern Kyndryl der Einhaltung der DSP in einem schriftlichen Vertrag zwischen Kyndryl und dem Kunden ausdrücklich zugestimmt hat. Zur Klarstellung: Diese Maßnahmen finden keine Anwendung, wenn der Kunde für Sicherheit und Datenschutz selbst verantwortlich ist oder nachstehend bzw. in einem Kyndryl Servicedokument festgelegte Bedingungen gelten.

a. Der Kunde ist dafür verantwortlich, festzustellen, ob ein Kyndryl Service für die Verwendung durch den Kunden geeignet ist, und Sicherheits- und Datenschutzmaßnahmen für Komponenten zu implementieren und zu verwalten, die Kyndryl nicht im Rahmen der Kyndryl Services bereitstellt oder verwaltet. Beispiele für Verantwortlichkeiten des Kunden in Bezug auf Kyndryl Services umfassen unter anderem: (1) Sicherheit von Systemen und Anwendungen, die der Kunde auf einem Infrastructure-as-a-Service- oder Platform-as-a-Service-Angebot oder auf einer Infrastruktur, Komponenten oder Software erstellt oder bereitstellt, die Kyndryl für einen Kunden verwaltet, und (2) Zugriffssteuerung für Endbenutzer des Kunden und Sicherheitskonfiguration auf Anwendungsebene für ein Software-as-a-Service-Angebot, das Kyndryl für einen Kunden verwaltet, oder für ein Anwendungsservice-Angebot, das Kyndryl einem Kunden bereitstellt.

b. Der Kunde bestätigt, dass Kyndryl diese DSP von Zeit zu Zeit nach eigenem Ermessen ändern kann und diese Änderungen vorherige Versionen ab dem Zeitpunkt ersetzen, an dem Kyndryl die geänderte Version veröffentlicht. Ungeachtet gegenteiliger Regelungen in einem schriftlichen Vertrag zwischen Kyndryl und dem Kunden wird mit einer Änderung Folgendes beabsichtigt: (1) Verbesserung oder Klarstellung bestehender Verpflichtungen, (2) Unterstützung von Kyndryl bei der angemessenen Priorisierung seines Sicherheitsschwerpunkts auf die Behebung entstehender Bedrohungen und Probleme für Daten und Cybersicherheit, (3) Aufrechterhaltung der Abstimmung auf aktuelle Normen und geltendes Recht oder (4) Bereitstellung zusätzlicher Features und

Funktionen. Durch Änderungen werden die Sicherheits- oder Datenschutzfeatures oder -funktionen von Kyndryl Services nicht eingeschränkt.

c. Bei Widersprüchen zwischen diesen DSP und einem Kyndryl Servicedokument hat das Kyndryl Servicedokument Vorrang. Stammen die widersprechenden Vertragsbedingungen aus einem Auftragsdokument, setzen diese die Bedingungen dieser DSP außer Kraft und gelten nur für die zutreffende Transaktion.

3. Datenschutz

a. Kyndryl wird sämtliche Inhalte vertraulich behandeln, indem die Inhalte nur Mitarbeitern, Auftragnehmern und Lieferanten (einschließlich Unterauftragsverarbeitern) von Kyndryl und ausschließlich in dem Umfang offengelegt werden, der zur Bereitstellung der Kyndryl Services erforderlich ist.

b. Sicherheits- und Datenschutzmaßnahmen für jeden einzelnen Kyndryl Service werden in Übereinstimmung mit den Verfahren für Sicherheit und Datenschutz durch Technikgestaltung von Kyndryl implementiert, um Inhalte zu schützen, die durch einen Kyndryl Service verarbeitet werden, und um die Verfügbarkeit dieser Inhalte gemäß dem anwendbaren schriftlichen Vertrag zwischen Kyndryl und dem Kunden, einschließlich zutreffender Kyndryl Servicedokumente, sicherzustellen.

c. Zusätzliche spezielle Sicherheits- und Datenschutzinformationen für einen Kyndryl Service sind ggf. im zutreffenden Kyndryl Servicedokument oder in anderen Standarddokumenten enthalten, um eine erste und fortlaufende Bewertung der Eignung eines Kyndryl Service für die Verwendung durch den Kunden zu unterstützen. Diese Informationen können Nachweise von Zertifizierungen und Akkreditierungen, Informationen in Verbindung mit diesen Zertifizierungen und Akkreditierungen, Datenblätter, häufig gestellte Fragen und sonstige allgemein verfügbare Dokumente umfassen. Kyndryl wird den Kunden auf verfügbare Standarddokumente hinweisen, sofern dieser Fragebögen zu Sicherheit oder Datenschutz ausfüllen muss.

4. Sicherheitsrichtlinien

a. Kyndryl unterhält und befolgt schriftliche IT-Sicherheitsrichtlinien und -verfahren, die einen integralen Bestandteil der Geschäftstätigkeit von Kyndryl darstellen und für alle Kyndryl Mitarbeiter verbindlich sind. Der Kyndryl Chief Information Security Officer bleibt verantwortlich für diese Richtlinien, einschließlich formaler Governance und Überarbeitungsmanagement, Mitarbeiterschulung und Durchsetzung der Compliance.

b. Kyndryl wird seine IT-Sicherheitsrichtlinien mindestens einmal jährlich überprüfen und in dem Umfang ändern, den Kyndryl für die Aufrechterhaltung des Schutzes von Kyndryl Services und Inhalten für angemessen hält.

c. Kyndryl wird seine verbindlichen Standardanforderungen in Bezug auf die Überprüfung aller neu eingestellten Beschäftigten aufrechterhalten und befolgen und diese Anforderungen auf seine 100-prozentigen Tochtergesellschaften ausweiten. Diese Anforderungen werden gemäß den internen Prozessen und Verfahren von Kyndryl regelmäßig überprüft und können unter anderem die Überprüfung möglicher Vorstrafen und der Identität sowie zusätzliche Prüfungen umfassen, die von Kyndryl als notwendig erachtet werden. Jede Kyndryl Gesellschaft ist für die Umsetzung dieser Anforderungen im Rahmen ihres Einstellungsverfahrens verantwortlich, sofern diese anwendbar und unter der jeweils geltenden Rechtsordnung zulässig sind.

d. Kyndryl Mitarbeiter werden jährlich Schulungen für Sicherheit und Datenschutz absolvieren und jedes Jahr nachweisen, dass sie die Anforderungen von Kyndryl in Bezug auf Unternehmensethik, Vertraulichkeit und Sicherheitsrichtlinien gemäß den Angaben in den Kyndryl Geschäftsgrundsätzen (Business Conduct Guidelines) einhalten. Personen mit privilegiertem Zugriff auf Komponenten erhalten zusätzliche Schulungen, die speziell auf ihre Rolle beim Betrieb und Support der Kyndryl Services abgestimmt sind, und soweit erforderlich, um Compliance und Akkreditierungen gemäß den Angaben im zutreffenden Kyndryl Servicedokument sicherzustellen.

5. Compliance

a. Kyndryl wird Compliance und Akkreditierung für die Kyndryl Services gemäß Definition in einem Kyndryl Servicedokument sicherstellen.

b. Auf Anforderung wird Kyndryl Nachweise für die im Rahmen von Ziffer 5.a. erforderliche Compliance und Akkreditierung bereitstellen, wie z. B. Zertifikate, Beglaubigungen oder Berichte aus

akkreditierten, unabhängigen Audits Dritter (akkreditierte, unabhängige Audits Dritter finden in der geforderten Häufigkeit der zutreffenden Norm statt).

c. Kyndryl ist für diese Datensicherheits- und Datenschutzmaßnahmen verantwortlich, selbst wenn Kyndryl einen Auftragnehmer oder Lieferanten (einschließlich Unterauftragnehmer) für die Bereitstellung oder Unterstützung eines Kyndryl Service einsetzt.

6. Sicherheitsvorfälle

a. Kyndryl wird dokumentierte Richtlinien für die Reaktion auf Sicherheitsvorfälle vorweisen und befolgen, die den Richtlinien des National Institute of Standards and Technology des US-Handelsministeriums (NIST) oder gleichwertigen Branchenstandards für die Abwicklung von IT-Sicherheitsvorfällen entsprechen, und die Bedingungen des anwendbaren schriftlichen Vertrags zwischen Kyndryl und dem Kunden in Bezug auf die Benachrichtigung bei Datenschutzverletzungen einhalten.

b. Kyndryl wird Sicherheitsvorfälle, die Kyndryl bekannt werden, untersuchen und im Rahmen der Kyndryl Services einen entsprechenden Reaktionsplan definieren und ausführen. Der Kunde kann Kyndryl über eine mutmaßliche Schwachstelle oder einen mutmaßlichen Vorfall informieren, indem er über den für den Kyndryl Service spezifischen Berichtsprozess für Sicherheitsvorfälle eine Anforderung einreicht (gemäß den Angaben in einem Kyndryl Servicedokument) oder, sofern es keinen solchen Prozess gibt, eine Anforderung für technische Unterstützung übermittelt.

c. Kyndryl wird den Kunden unverzüglich informieren, wenn ein Sicherheitsvorfall bestätigt wird, der bekanntermaßen oder nach Vermutung von Kyndryl Auswirkungen auf den Kunden haben wird. Kyndryl wird dem Kunden alle angeforderten Informationen über einen solchen Sicherheitsvorfall und den Status von Korrektur- und Wiederherstellungsaktivitäten durch Kyndryl in angemessenem Umfang bereitstellen.

7. Physische Sicherheit und Zutrittskontrolle

a. Kyndryl wird angemessene physische Zutrittskontrollen, wie z. B. Absperrungen, kartengesteuerte Eingangspunkte, Überwachungskameras und besetzte Empfangsschalter, bereitstellen, um die von Kyndryl verwalteten Einrichtungen (Rechenzentren) für das Hosting der Kyndryl Services vor unbefugtem Zutritt zu schützen. Externe Eingangspunkte zu diesen Rechenzentren, wie z. B. Zustellbereiche und Ladedocks, werden entsprechend kontrolliert und von IT-Ressourcen isoliert.

b. Der Zutritt zu von Kyndryl verwalteten Rechenzentren und kontrollierten Bereichen in diesen Rechenzentren ist nach Aufgabenbereich beschränkt und unterliegt einer Genehmigung. Der Zutritt wird protokolliert und die Protokolle werden für einen Zeitraum von mindestens einem Jahr aufbewahrt. Kyndryl widerruft den Zutritt zu von Kyndryl verwalteten Rechenzentren nach Kündigung eines autorisierten Mitarbeiters. In diesem Zusammenhang hält Kyndryl die formal dokumentierten Kündigungsverfahren ein, die eine unverzügliche Entfernung des Mitarbeiters aus den Zutrittskontrolllisten und Rückgabe von Ausweisen für den physischen Zutritt umfassen.

c. Alle Personen, die eine temporäre Zutrittsberechtigung zu einem von Kyndryl verwalteten Rechenzentrum oder einem kontrollierten Bereich in einem solchen Rechenzentrum erhalten, werden beim Zutritt zu den Räumlichkeiten registriert, müssen bei der Registrierung einen Identitätsnachweis bereitstellen und werden von autorisiertem Personal begleitet. Alle temporären Zutrittsberechtigungen, einschließlich Anlieferung, werden im Voraus geplant und erfordern die Genehmigung durch autorisiertes Personal.

d. Kyndryl wird entsprechende Vorkehrungen treffen, um die physische Infrastruktur der von Kyndryl verwalteten Rechenzentren vor Umweltgefahren, sowohl natürlicher als auch vom Menschen verursachter Gefahren, wie z. B. überhöhte Umgebungstemperaturen, Brände, Hochwasser, Feuchtigkeit, Diebstahl und Vandalismus, zu schützen.

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

a. Kyndryl wird die Sicherheitsarchitektur für Komponenten überprüfen. Dies schließt Maßnahmen zur Vermeidung von unbefugten Netzverbindungen zu Systemen, Anwendungen und Netzeinheiten ein, um die eigenen Standards für sichere Segmentierung, Isolation und tiefengestaffelte Sicherheit vor der Implementierung einzuhalten.

b. Kyndryl kann für die Wartung und Unterstützung der Kyndryl Services und zugehörigen Komponenten drahtlose Netztechnologie einsetzen. Diese drahtlosen Netze werden ggf. verschlüsselt und erfordern eine sichere Authentifizierung.

c. Kyndryl wird Maßnahmen für einen Kyndryl Service bereitstellen, die konzipiert sind, um Inhalte logisch voneinander zu trennen und zu verhindern, dass diese Unbefugten gegenüber offengelegt oder diesen zugänglich werden. Kyndryl wird eine angemessene Isolation seiner für die Produktion verwendeten Umgebungen und seiner nicht für die Produktion verwendeten Umgebungen sicherstellen. Falls Inhalte in eine nicht für die Produktion verwendete Umgebung übertragen werden, beispielsweise, um auf Anforderung des Kunden einen Fehler zu reproduzieren, müssen Sicherheit und Datenschutz in der nicht für die Produktion verwendeten Umgebung denen in der für die Produktion verwendeten Umgebung entsprechen.

d. Kyndryl wird Inhalte, die weder für öffentliche noch nicht authentifizierte Einsicht vorgesehen sind, bei der Übertragung über öffentliche Netze verschlüsseln und die Verwendung eines Verschlüsselungsprotokolls wie HTTPS, SFTP oder FTPS für die sichere Übertragung von Inhalten des Kunden an und von Kyndryl Services über öffentliche Netze unterstützen.

e. Kyndryl wird ruhende Inhalte gemäß den Angaben in einem Kyndryl Servicedokument verschlüsseln, falls erforderlich. Sollte ein Kyndryl Service das Management von Verschlüsselungsschlüsseln umfassen, wird Kyndryl dokumentierte Verfahren für Generierung, Ausgabe, Verteilung, Speicherung, Rotation, Widerruf, Wiederherstellung, Sicherung, Vernichtung, Zugriff auf und Verwendung von Sicherheitsschlüsseln bereitstellen.

f. Falls Kyndryl Zugriff auf Inhalte benötigt, um die Kyndryl Services bereitzustellen, und falls dieser Zugriff von Kyndryl verwaltet wird, wird Kyndryl den Zugriff auf das erforderliche Minimum beschränken. Dieser Zugriff sowie der Verwaltungszugriff auf zugrunde liegende Komponenten (privilegierter Zugriff) sind individuell, rollenbasiert und unterliegen der Genehmigung und regelmäßigen Validierung durch autorisiertes Kyndryl Personal in Übereinstimmung mit den Prinzipien der Aufgabentrennung. Kyndryl wird Maßnahmen bereitstellen, um redundante und inaktive Konten mit privilegiertem Zugriff zu identifizieren und zu entfernen, und diesen Zugriff nach Kündigung des Kontoinhabers oder auf Anforderung von autorisiertem Kyndryl Personal, z. B. dem Manager des Kontoinhabers, unverzüglich widerrufen.

g. In Übereinstimmung mit Verfahren gemäß Branchenstandard und soweit von den einzelnen Komponenten nativ unterstützt, wird Kyndryl technische Maßnahmen bereitstellen, die ein Zeitlimit für inaktive Sitzungen, eine Sperrung von Konten nach mehreren aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen, eine Authentifizierung durch sichere Kennwörter oder Kennphrasen, eine bestimmte Häufigkeit von Kennwortänderungen und eine sichere Übertragung und Speicherung dieser Kennwörter und Kennphrasen durchsetzen.

h. Kyndryl wird die Verwendung von privilegiertem Zugriff überwachen und Sicherheitsinformationen sowie Maßnahmen für das Ereignismanagement zu folgenden Zwecken bereitstellen: (1) Ermittlung von unbefugtem Zugriff und unbefugten Aktivitäten, (2) Vereinfachung einer rechtzeitigen und angemessenen Reaktion und (3) Unterstützung von internen Audits und Audits unabhängiger Dritter in Verbindung mit der Einhaltung der dokumentierten Kyndryl Richtlinie.

i. In Übereinstimmung mit der Richtlinie von Kyndryl werden Protokolle aufbewahrt, in denen privilegierter Zugriff und privilegierte Aktivitäten aufgezeichnet werden. Kyndryl wird entsprechende Maßnahmen bereitstellen, um Schutz vor unbefugtem Zugriff auf solche Protokolle, deren Änderung und zufälliger oder absichtlicher Vernichtung zu bieten.

j. Soweit unterstützt durch native Geräte- oder Betriebssystemfunktionalität, wird Kyndryl Schutzvorkehrungen für die Datenverarbeitung für Endbenutzersysteme bereitstellen, die unter anderem Endpunktfirewalls, vollständige Plattenverschlüsselung, Erkennung und Entfernung von Malware, zeitbasierte Bildschirmsperren und Endpunktmanagementlösungen zur Durchsetzung von Anforderungen hinsichtlich Sicherheitskonfiguration und Patching umfassen können.

k. Kyndryl wird physische Medien, die wiederverwendet werden sollen, vor einer solchen Wiederverwendung sicher bereinigen, und physische Medien, die nicht wiederverwendet werden sollen, in Übereinstimmung mit NIST-Richtlinien für die Medienbereinigung vernichten.

9. Serviceintegritäts- und Verfügbarkeitskontrolle

a. Kyndryl wird Folgendes durchführen: (1) Sicherheits- und Datenschutzrisikobewertungen der Kyndryl Services mindestens einmal jährlich, (2) Sicherheitstests und Schwachstellenanalysen der Kyndryl

Services vor der Produktionsfreigabe und danach mindestens einmal jährlich, (3) Penetrationstests für Funktionen und Angebote vor Produktionsfreigabe und danach jährlich, (4) automatisierte Schwachstellensuche bei zugrunde liegenden Komponenten der Kyndryl Services im Vergleich zu branchenspezifischen Best Practices für die Sicherheitskonfiguration, (5) Behebung identifizierter Schwachstellen aus Sicherheitstests und Scans basierend auf zugeordneten Risiken, Exploit-Anfälligkeiten und Auswirkungen sowie (6) Einleiten angemessener Schritte zur Vermeidung von Störungen der Kyndryl Services bei der Durchführung von Tests, Bewertungen, Scans und Korrekturen.

b. Kyndryl wird Maßnahmen bereitstellen, um Sicherheitspatches für die Kyndryl Services und zugeordneten Systeme, Netze, Anwendungen und zugrunde liegenden Komponenten im Rahmen der Kyndryl Services zu bewerten, zu testen und anzuwenden. Sobald festgestellt wird, dass ein Sicherheitspatch anwendbar und angemessen ist, wird Kyndryl das Patch in Übereinstimmung mit den dokumentierten Richtlinien für die Dringlichkeits- und Risikobewertung ggf. basierend auf den Bewertungen des Common Vulnerability Scoring Systems von Patches implementieren. Für die Implementierung von Sicherheitspatches gilt die Kyndryl Änderungsmanagementrichtlinie.

c. Kyndryl wird Richtlinien und Verfahren für Risikomanagement in Verbindung mit der Anwendung von Änderungen an Kyndryl Services bereitstellen. Vor der Implementierung werden Änderungen an einem Kyndryl Service, einschließlich seiner Systeme, Netze und zugrunde liegenden Komponenten, in einer registrierten Änderungsanforderung dokumentiert, die eine Beschreibung der Änderung und den Grund für die Änderung, Details und Zeitplan der Implementierung, eine Risikodarstellung mit Auswirkungen auf den Kyndryl Service und seine Kunden, erwartetes Ergebnis, Rollback-Plan sowie dokumentierte Genehmigung durch autorisiertes Personal umfasst.

d. Kyndryl wird einen Bestand sämtlicher IT-Assets, die beim Betrieb der Kyndryl Services verwendet werden, führen. Zudem wird Kyndryl fortlaufend den Zustand, einschließlich Kapazität und Verfügbarkeit von Kyndryl Services und zugrunde liegenden Komponenten überwachen und verwalten.

e. Jeder Kyndryl Service wird mittels Business-Impact-Analyse und Risikobewertungen zur Identifizierung und Priorisierung kritischer Geschäftsfunktionen separat in Bezug auf Anforderungen hinsichtlich Business-Continuity und Disaster-Recovery bewertet. Für jeden Kyndryl Service wird es, soweit durch die Risikobewertungen sichergestellt, separat definierte, dokumentierte, bereitgestellte und jährlich validierte Business-Continuity- und Disaster-Recovery-Pläne geben, die mit den Verfahren gemäß Branchenstandard übereinstimmen. Zielsetzungen für Recovery-Punkt und -Zeit für einen Kyndryl Service, sofern im zutreffenden Kyndryl Servicedokument vorgesehen, werden unter Berücksichtigung der Architektur und bestimmungsgemäßen Verwendung des Kyndryl Service festgelegt. Physische Medien, die zur Auslagerung an einen anderen Standort vorgesehen sind, wie z. B. Medien mit Sicherungsdateien, werden vor dem Transport verschlüsselt.