SAAS-SICHERHEITSANHANG

Einleitung: Hyland unterhält und verwaltet ein umfassendes schriftliches Sicherheitsprogramm, das den Hyland Cloud-Dienst abdeckt und zum Schutz: (a) der Sicherheit und Integrität der Kundendaten; (b) vor Bedrohungen und Gefahren, die sich negativ auf die Kundendaten auswirken können; und (c) vor unbefugtem Zugriff auf die Kundendaten, dient. Dieses Programm umfasst Folgendes :

1. Risikomanagement.
    a. Durchführung einer jährlichen Risikobewertung um Bedrohungen und Schwachstellen in den administrativen, physischen, rechtlichen, behördlichen und technischen Sicherheitsvorkehrungen zu identifizieren, die zum Schutz des Hyland Cloud-Dienstes eingesetzt werden.
    b. Aufrechterhaltung eines dokumentierten Risikosanierungsprozesses, um die Verantwortung für identifizierte Risiken zuzuweisen, Sanierungspläne und Zeitrahmen festzulegen und eine regelmäßige Überwachung des Fortschritts zu gewährleisten.
2. Informationssicherheitsprogramm.
    a. Aufrechterhaltung eines dokumentierten, umfassenden Informationssicherheitsprogramms für den Hyland Cloud-Dienst. Dieses Programm umfasst Richtlinien und Verfahren, die auf Industriestandards basieren, wie z. B. ISO 27001/27002 oder anderen gleichwertige Standards.
    b. Ein solches Informationssicherheitsprogramm muss, gegebenenfalls, Folgendes umfassen: (i) angemessene physische Sicherheit und Cybersicherheit an den Orten, an denen Kundendaten verarbeitet und/oder gespeichert werden; und (ii) angemessene Vorsichtsmaßnahmen in Bezug auf die Beschäftigung von Hyland-Mitarbeitern.
    c. Diese Richtlinien werden jährlich vom Hyland-Management überprüft und aktualisiert.
3. Organisation der Informationssicherheit. Zuweisung von Sicherheitsverantwortlichkeiten an geeignete Hyland-Einzelpersonen oder -Gruppen, um den Schutz des Hyland Cloud-Dienstes und der damit verbundenen Vermögenswerte zu erleichtern.
4. Sicherheit im Personalwesen.
    a. Hyland-Mitarbeiter werden während des Einstellungsprozesses einer umfassenden Prüfung unterzogen. Es werden Hintergrundüberprüfungen und Referenzvalidierungen durchgeführt, um festzustellen, ob die Qualifikationen des Kandidaten für die vorgeschlagene Position geeignet sind. Vorbehaltlich jeglicher Einschränkungen, die durch geltendes Recht auferlegt werden und auf der Grundlage der Rechtsprechung, umfassen diese Hintergrundüberprüfungen gegebenenfalls eine strafrechtliche Hintergrundüberprüfung, eine überprüfung der vorhergehender Beschäftigungen und der Ausbildung.
    b. Sicherstellung, dass alle Hyland-Mitarbeiter einer Vertraulichkeits- und Geheimhaltungsverpflichtung unterliegen, bevor der Zugriff auf den Hyland Cloud-Dienst oder die Kundendaten bereitgestellt wird.
    c. Sicherstellung, dass alle Hyland-Mitarbeiter eine Sicherheitsbewusstseinsschulung erhalten, welche diesen Mitarbeitern Kenntnisse zur Informationssicherheit vermittelt, um die Sicherheit, Verfügbarkeit und Vertraulichkeit der Kundendaten zu gewährleisten.
    d. Nach dem Ausscheiden eines Hyland-Mitarbeiters oder einem Rollenwechsel stellt Hyland sicher, dass der Zugriff eines Hyland-Mitarbeiters auf den Hyland Cloud-Dienst zeitnah widerrufen wird und alle anwendbaren Hyland-Vermögenswerte, sowohl Informationen als auch physische Werte, zurückgegeben werden.
5. Vermögensverwaltung.

a. Aufrechterhaltung von Richtlinien und Verfahren zur Verwaltung von Vermögenswerten und Informationen. Dies umfasst Eigentumsrechte an Vermögenswerten, eine Bestandsaufnahme von Vermögenswerten, Klassifizierungsrichtlinien und Handhabungsstandards für Hyland-Vermögenswerte.

b. Aufrechterhaltung von Verfahren zur Handhabung von Medien, um sicherzustellen, dass Medien, die Kundendaten als Teil des Hyland Cloud-Dienstes enthalten, verschlüsselt und an einem sicheren Ort aufbewahrt werden, der strengen physischen Zugangskontrollen unterliegt.

c. Wenn ein Hyland Cloud-Dienst-Speichergerät das Ende seiner Nutzungsdauer erreicht hat, beinhalten die Verfahren einen Stilllegungsprozess, der verhindern soll, dass Kundendaten unbefugten Personen zugänglich gemacht werden, in dem die von NIST empfohlenen Techniken zur Datenvernichtung als Teil des Stilllegungsprozesses angewendet werden.

d. Wenn ein Hyland-Speichergerät mit diesen Verfahren außer Betrieb genommen werden kann, wird das Gerät virtuell geschreddert, entmagnetisiert, bereinigt/gelöscht oder physisch zerstört, in Übereinstimmung mit branchenüblichen Verfahren.

6. Zugriffskontrollen.

a. Aufrechterhaltung einer logischen Zugriffsrichtlinie und entsprechender Verfahren. Die Verfahren für den logischen Zugriff definieren den Antrags-, Genehmigungs- und Zugriffsprozess für Hyland-Mitarbeiter. Der logische Zugriffsprozess beschränkt den Zugriff von Hyland-Benutzern (lokal und remote) basierend auf der Arbeitsfunktion des Hyland-Benutzers (rollen-/profilbasiert, angemessener Zugriff) für Anwendungen und Datenbanken. Der Zugriff der Hyland-Benutz wird in regelmäßigen Abständen rezertifiziert, um Zugriffe und Privilegien zu bestimmen. Die Verfahren für den Einstellungs- und Kündigungsprozess von Hyland-Mitarbeitern in einer zeitgemässen Weise werden dokumentiert. Die Verfahren für die Inaktivitätsschwelle des Hyland-Mitarbeiters, welche zu einer Kontosperrung und -entfernung führt, werden dokumentiert.

b. Beschränkung des Zugriffs von Hyland-Mitarbeitern auf Kundendaten, die den Zugriff auf die Kundendaten als Voraussetzung für die Erbringung der Leistungen von Hyland im Rahmen dieser Vereinbarung benötigen. Hyland wendet das Prinzip des „geringsten Privilegs“ und das Konzept des „minimal Notwendigen“ an, um den Grad des Zugriffs aller Hyland-Benutzer auf Kundendaten zu bestimmen. Hyland verlangt sichere Passwörter, die den Komplexitätsanforderungen und der regelmäßigen Rotation unterliegen, sowie die Verwendung der Multi-Faktor-Authentifizierung.

c. Sicherstellung, dass strenge Zugriffskontrollen für den Zugriff auf Kundendaten durch Hyland vorhanden sind. Die Administratoren des Kunden kontrollieren den Benutzerzugriff, die Benutzerberechtigungen und die Aufbewahrung der Kundendaten in dem Umfang, in dem solche Kontrollen für den Kunden in Bezug auf den Hyland Cloud-Dienst zur Verfügung stehen.

7. Systemgrenzen.

a. Hyland ist nicht verantwortlich für Systemkomponenten, die sich nicht innerhalb der Hyland Cloud Plattform befinden, einschließlich Netzwerkgeräte, Netzwerkverbindungen, Workstations, Server und Software, die im Besitz des Kunden oder Dritter sind und von diesen betrieben werden. Hyland kann nach eigenem Ermessen Unterstützung für diese Komponenten anbieten.

b. Die innerhalb der Hyland Cloud Plattform ausgeführten Prozesse beschränken sich auf diejenigen, die von einem Hyland-Mitarbeiter (oder einem von Hyland autorisierten Dritten) ausgeführt werden, oder auf Prozesse, die in ihrer Gesamtheit innerhalb der etablierten Systemgrenzen von Hyland ausgeführt werden. Dies beinhaltet, ist aber nicht beschränkt auf, Hardware-Installation, Software-Installation, Datenreplikation, Datensicherheit und Authentifizierungsprozesse.

c. Bestimmte Geschäftsprozesse können diese Grenzen überschreiten, d.h. eine oder mehrere Aufgaben werden außerhalb der von Hyland festgelegten Systemgrenzen für die Hyland Cloud Plattform ausgeführt, eine oder mehrere Aufgaben werden von Personen ausgeführt, die keine Hyland-Mitarbeiter (oder autorisierte Dritte) sind, oder einer oder mehrere Aufgaben werden auf der Grundlage schriftlicher Anfragen des Kunden

ausgeführt. In einem solchen Fall wird Hyland Unterstützung für solche Prozesse leisten, soweit sie innerhalb der von Hyland festgelegten Systemgrenzen auftreten. Hyland ist jedoch nicht dafür verantwortlich, solche Prozesse zu leisten, sofern sie außerhalb dieser festgelegten Systemgrenzen auftreten. Hyland kann nach eigenem Ermessen begrenzte Unterstützung für solche Prozesse bereitstellen, die außerhalb dieser festgelegten Systemgrenzen für die Hyland Cloud Plattform auftreten. Beispiele für Geschäftsprozesse, die diese Grenzen überschreiten, sind unter anderem Konfigurationsänderungen des Hyland Cloud-Dienstes, Verarbeitungen, die innerhalb des Hyland Cloud-Dienstes stattfinden, Benutzerautorisierung und Dateiübertragungen.

8. Verschlüsselung.

    a. Kundendaten dürfen nur in einem verschlüsselten Format, wie z. B. SFTP, TLS / SSL oder einer anderen gleichwertigen Methode im Hyland Cloud-Dienst hochgeladen werden.

    b. Die Kundendaten werden im Ruhezustand verschlüsselt.

    c. Wenn die Verwendung der Verschlüsselungsfunktionalität vom Kunden kontrolliert oder geändert werden kann und der Kunde die Verwendung der Verschlüsselungsfunktionalität ändern oder deaktivieren möchte, geschieht dies beim Kunden auf eigenes Risiko.

9. Physische Sicherheit und Umgebungssicherheit.

    a. Die Hyland Cloud Plattform verwendet Rechenzentren oder Drittanbieter, die die Einhaltung eines oder mehrerer der folgenden Standards (oder eines angemessenen Äquivalents) nachgewiesen haben: International Organization for Standardization („ISO“) 27001 und/oder des American Institute of Certified Public Accountants („AICPA“), Service Organization Controls („SOC“) Berichte für Serviceorganisationen. Diese Anbieter stellen Internetverbindungen, physische Sicherheit, Strom- und Umgebungssysteme sowie andere Dienste für die Hyland Cloud Plattform bereit.

    b. Hyland verwendet Architektur und Technologien, welche darauf ausgelegt sind, sowohl Sicherheit als auch hohe Verfügbarkeit zu fördern.

10. Betriebssicherheit.

    a. Aufrechterhaltung der dokumentierten Hyland Cloud-Betriebsverfahren.

    b. Aufrechterhaltung von Change Management Kontrollen, um sicherzustellen, dass von Hyland vorgenommene Änderungen an den Hyland Cloud-Dienst Produktionssystemen vor der Implementierung ordnungsgemäss autorisiert und überprüft werden. Der Kunde ist dafür verantwortlich, alle Konfigurationsänderungen, Authentifizierungsänderungen und Upgrades, die vom Kunden oder von Hyland auf Anfrage des Kunden implementiert werden, vor der Produktionsnutzung des Hyland Cloud-Dienstes zu testen. In Fällen, in denen sich der Kunde darauf verlässt, dass Hyland Änderungen in seinem Namen vornimmt, muss eine schriftliche Anfrage, die die Änderung beschreibt (z. B. eine E-Mail oder eine andere von Hyland bereitgestellte Methode), von den vom Kunden benannten Customer Security Administrators („CSAs“) eingereicht oder in einem Dienstleistungsangebot dargelegt werden. Hyland wird während eines geplanten Wartungsfensters Konfigurationsänderungen vornehmen, die sich voraussichtlich auf den Zugriff des Kunden auf seinen Hyland Cloud-Dienst auswirken werden. Hyland darf Konfigurationsänderungen, bei denen keine Auswirkungen auf den Kunden zu erwarten sind, während der normalen Geschäftszeiten vornehmen.

    c. Überwachung der Nutzung und des Kapazitätsniveaus innerhalb der Hyland Cloud Plattform, um zukünftiges Wachstum angemessen und proaktiv zu planen.

    d. Verwendung von Viren- und Malware-Schutztechnologien, die so konfiguriert sind, dass sie den gängigen Industriestandards entsprechen, um die Kundendaten und Geräte in der Hyland Cloud Plattform vor Virusinfektionen oder ähnlichen Malicious Payloads zu schützen.

    e. Implementierung von Disaster Recovery- und Business Continuity-Verfahren. Dazu gehört die Replikation von

Kundendaten an einen sekundären Speicherort.

f. Aufrechterhaltung eines System- und Sicherheitsprotokollierungsprozesses zur Erfassung von Systemprotokollen, die von Hyland als kritisch eingestuft werden. Diese Protokolle müssen mindestens sechs Monate lang aufbewahrt und regelmäßig überprüft werden.

g. Aufrechterhaltung von Systemhärtungsanforderungen und Konfigurationsstandards für Komponenten, die in der Hyland Cloud Plattform bereitgestellt werden. Sicherstellen, dass Server, Betriebssysteme und unterstützende Software, die in der Hyland Cloud Plattform verwendet werden, alle kritischen und Hochsicherheitspatches rechtzeitig erhalten, jedoch in keinem Fall mehr als 90 Tage nach der Veröffentlichung, vorbehaltlich des nächsten Satzes. Für den Fall, dass ein solcher Sicherheitspatch den Hyland Cloud-Dienst erheblich beeinträchtigen würde, wird Hyland angemessene Anstrengungen unternehmen, um Ausgleichskontrollen zu implementieren, bis ein Sicherheitspatch verfügbar ist, der den Hyland Cloud-Dienst nicht wesentlich beeinträchtigt.

h. Mindestens vierteljährliche Durchführung von Schwachstellen-Scans oder -Analysen der Hyland Cloud Plattform und Behebung aller identifizierten kritischen und hochgradigen Schwachstellen, in Übereinstimmung mit seinen Patch-Management-Verfahren.

i. Mindestens jährliche Durchführung von Penetrationstests der Hyland Cloud Plattform.

11. Kommunikationssicherheit

    a. Implementierung von Sicherheitskontrollen für die Hyland Cloud Plattform zum Schutz von Informationsressourcen innerhalb der Hyland Cloud Plattform.

    b. Wenn unterstützt, kann der Kunde bei der Implementierung und danach einmal jährlich verlangen, dass Hyland den Zugriff auf den Hyland Cloud-Dienst des Kunden ohne zusätzliche Kosten auf eine Liste von vordefinierter IP-Adressen beschränkt.

12. Lieferantenbeziehungen. Aufrechterhaltung eines Lieferantenverwaltungsprogramms für seine kritischen Lieferanten. Dieses Programm stellt sicher, dass kritische Lieferanten auf jährlicher Basis bewertet werden.

13. Sicherheitsvorfall.

    a. Anwendung von Standards zur Reaktion auf Vorfälle, die auf anwendbaren Industriestandards basieren, wie z.B. ISO 27001:2013 und dem Nationalen Institut for Standards and Technology („NIST"), um die Informationssicherheitskomponenten der Hyland Cloud-Dienst-Umgebung aufrechtzuerhalten.

    b. Die Reaktionen auf solche Vorfälle folgen der von Hyland dokumentierten Reaktionssequenz auf Vorfälle. Diese Sequenz umfasst die Auslösephase des Vorfalls, die Bewertungsphase, die Eskalationsphase, die Reaktionsphase, die Wiederherstellungsphase, die Deeskalationsphase und die Überprüfungsphase nach dem Vorfall.

    c. Wenn Hyland festgestellt, dass der Hyland Cloud-Dienst des Kunden durch einen Sicherheitsvorfall negativ beeinflusst wurde, wird Hyland eine Zusammenfassung der Ursachenanalyse liefern. Eine solche Benachrichtigung wird nicht unangemessen verzögert, sondern erfolgt, nachdem erste Korrekturmaßnahmen ergriffen wurden, um die Sicherheitsbedrohung einzudämmen oder den Hyland Cloud-Dienst zu stabilisieren.

    d. Die Ursachenanalyse umfasst die Dauer des Ereignisses, die Lösung, die technische Zusammenfassung, ausstehende Probleme und Folgemassnahmen, einschließlich der Schritte, die der Kunde unternehmen muss, um weitere Probleme zu vermeiden. Die Informationen des Hyland Cloud-Dienstes, einschließlich der Datenelemente, die zusätzliche Vertraulichkeits- und Sicherheitsmaßnahmen erfordern (einschließlich derjenigen anderer Kunden, die von dem Ereignis betroffen sind), werden nicht öffentlich bekannt gegeben. Wenn der Kunde zusätzliche Details zu einem Vorfall benötigt, muss eine Anfrage an das Hyland GCS-Support-Team gestellt werden, die von Fall zu Fall bearbeitet wird. Der Prozess der Informationsfreigabe kann eine Überprüfung vor Ort erfordern, um die Vertraulichkeit und Sicherheit der angeforderten

Informationen zu schützen.

e. Hyland benachrichtigt den Kunden innerhalb von 48 Stunden über einen Sicherheitsvorfall. Ein „Sicherheitsvorfall" bedeutet, dass Hyland eine tatsächliche Offenlegung von unverschlüsselten Kundendaten gegenüber einer nicht autorisierten Person oder Organisation feststellt, welche die Sicherheit, Vertraulichkeit oder Integrität der Kundendaten gefährdet.

14. Informationssicherheitsaspekte des Business Continuity Managements.

    a. Aufrechterhaltung eines Business Continuity- und Disaster Recovery-Plans.

    b. Jährliche Überprüfung und Testung dieses Plans.

15. Aggregierte Daten.

    a. Hyland ist Eigentümer aller von Hyland gesammelten und verwendeten Kunden- und Benutzerregistrierungs- und Abrechnungsdaten, welche für die Einrichtung, Nutzung und Abrechnung des Hyland Cloud-Dienstes erforderlich sind („Kontoinformationen"), sowie aller aggregierten, anonymisierten und statistischen Daten, die aus der Nutzung und dem Betrieb des Hyland Cloud-Dienstes abgeleitet werden, insbesondere die Anzahl der Datensätze im Hyland Cloud-Dienst, die Anzahl und Art der Transaktionen, Konfigurationen und Berichte, die im Rahmen des Hyland Cloud-Dienstes verarbeitet werden, sowie die Leistungsergebnisse des Hyland Cloud-Dienstes (die "Aggregierten Daten").

    b. Hyland kann die Kontoinformationen und Aggregierten Daten für den Betrieb von Hyland verwenden. Zur Klarstellung: Kontoinformationen und Aggregierte Daten umfassen keine Kundendaten.

16. Sicherheitsanfrage.

    a. Die Überwachung der Einhaltung des Informationssicherheitsprogramms. Dies beinhaltet regelmäßige interne Überprüfungen. Die Ergebnisse werden mit dem Hyland-Management geteilt und Abweichungen werden bis zur Behebung verfolgt.

    b. Aufrechterhaltung eines regelmäßigen externen Prüfungsprogramms. Abgeschlossene Bescheinigungen, wie z. B. verfügbare SOC 2-Berichte, werden dem Kunden auf schriftliche Anfrage zur Verfügung gestellt.

    c. Der Kunde ist berechtigt, jährlich (jedoch nicht öfter als einmal innerhalb eines Zeitraums von 12 Monaten) Audits (einschließlich Bewertungen, Fragebögen, geführte Überprüfungen oder anderer Anfragen zur Validierung der Sicherheitskontrollen von Hyland; jeweils eine "Sicherheitsanfrage") der Hyland-Tätigkeiten durchzuführen, die an der laufenden Bereitstellung und Unterstützung des vom Kunden erworbenen Hyland Cloud-Dienstes beteiligt sind. Dies setzt voraus, dass der Kunde Hyland schriftlich vorab mitteilt, dass er eine solche Prüfung durchführen möchte und dass diese Sicherheitsanfrage sich nicht mit den gleichen oder ähnlichen Informationen oder dem Umfang von: (1) Kontrollen, die bereits in einer von Hyland durchgeführten externen Prüfung oder Bewertung vorgesehen sind (wie z. B. einem SOC 2-Bericht, ISO 27001 oder einer anderen ähnlichen Prüfung oder Bewertung), die dem Kunden auf Anfrage zur Verfügung gestellt wird, oder (2) Inhalten, die bereits von Hyland durch den ausgefüllten SIG-, CAIQ- oder ähnlichen Fragebogen dem Kunden auf Anfrage zur Verfügung gestellt werden, überschneidet. Für jede Sicherheitsanfrage gilt Folgendes: (1) Hyland und der Kunde vereinbaren einvernehmlich den Zeitpunkt, den Umfang und die Kriterien einer solchen Sicherheitsanfrage(dies kann unter den oben genannten Voraussetzungen das Ausfüllen der vom Kunden bereitgestellten Fragebögen beinhalten); (2) Dokumentation, die vertraulich oder zugangsbeschränkt ist (wie z. B. interne Richtlinien, Praktiken und Verfahren von Hyland, einschließlich der vom Kunden angeforderten Dokumentation, die aufgrund von physischen Einschränkungen oder Richtlinienbeschränkungen nicht aus den Räumlichkeiten von Hyland entfernt werden kann), wird nicht zur externen Ansicht zur Verfügung gestellt oder aus den Räumlichkeiten von Hyland entfernt; derartige Überprüfungen müssen vor Ort in der Unternehmenszentrale von Hyland in Ohio oder über eine sichere Bildschirmfreigabe durchgeführt werden, die von Hyland so eingerichtet werden kann, dass jede Art von Kopieren oder Screenshots verboten ist; (3) der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass Hyland keinen Zugriff auf interne Systeme oder Geräte gestattet, die zum Hosten oder Unterstützen der Hyland-Angebote verwendet werden; (4) sofern der Kunde einen Dritten mit der Durchführung einer solchen Sicherheitsanfrage beauftragen möchte, muss Hyland den Einsatz

dieses Dritten im Voraus schriftlich genehmigen; der Kunde muss diesen Dritten zudem dazu veranlassen, eine Geheimhaltungsvereinbarung mit Hyland abzuschließen und sich zur Einhaltung der Sicherheitsstandards von Hyland zu verpflichten; die Verwaltung der Zusammenarbeit mit diesem Dritten obliegt dem Kunden; der Kunde muss insbesondere sicherstellen, dass dem Dritte der zwischen Hyland und dem Kunden vereinbarte Umfang der Sicherheitsanfrage und die Nutzung der Hyland-Dienste durch den Kunden bekannt sind; und (5) der Kunde ist verpflichtet, Hyland Gebühren (zu Hyland's Standardtarifen) für die Dienstleistungen (einschließlich aller Auslagen und Kosten) zu zahlen , die von Hyland im Zusammenhang mit einer solchen Sicherheitsanfrage in Rechnung gestellt werden. Bei Bedarf wird Hyland in der Unternehmenszentrale von Hyland in Ohio private und angemessene Unterkünfte für Datenanalysen und Besprechungen bereitstellen. Hyland und der Kunde können nach angemessener Ankündigung einvernehmlich vereinbaren, die erforderlichen Mitarbeiter oder Auftragnehmer für persönliche oder telefonische Interviews während einer solchen Sicherheitsanfrage auf Kosten des Kunden zur Verfügung zu stellen. Dem Kunden ist es untersagt, die Ergebnisse dieser Sicherheitsanfrage ohne vorherige schriftliche Genehmigung von Hyland an Dritte weiterzugeben oder zu veröffentlichen. Der Kunde ist verpflichtet, diese Verpflichtung jeder Drittpartei, die an der Sicherheitsanfrage beteiligt ist, aufzuerlegen. Ungeachtet gegenteiliger Bestimmungen in dieser Vereinbarung verpflichtet nichts in dieser Vereinbarung (einschließlich dieses Abschnitts) Hyland oder eines seiner verbundenen Unternehmen zur Offenlegung von Informationen, die unter das Anwaltsgeheimnis fallen.