Die folgende Übersetzung dient nur zu Informationszwecken. Bei Abweichungen und Widersprüchlichkeiten zwischen dieser Übersetzung und der zuletzt aktualisierten englischen Fassung (einschließlich aufgrund von Übersetzungsverzögerungen) hat die englische Fassung Vorrang.

AMAZON-SICHERHEITSRICHTLINIEN FÜR ANBIETER

Letzte Aktualisierung: 11. September 2024

1. **GELTUNGSBEREICH.** Der Lieferant wird diese Sicherheitsanforderungen (die „Sicherheitsrichtlinie") einhalten. Diese Sicherheitsrichtlinie schränkt keine anderen vertraglichen oder gesetzlichen Verpflichtungen des Lieferanten ein. Soweit ein Konflikt zwischen dieser Sicherheitsrichtlinie und anderen Vereinbarungen zwischen dem Lieferanten und Amazon besteht, wird der Lieferant die restriktiveren Anforderungen einhalten, die die Amazon-Daten besser schützen.

2. **UPDATES**.

2.1 Amazon kann von Zeit zu Zeit geschäftlich angemessene Aktualisierungen dieser Sicherheitsrichtlinien vornehmen, die 30 Tage nach dem Datum der „letzten Aktualisierung" dieser Sicherheitsrichtlinie in Kraft treten. Der Lieferant erklärt sich damit einverstanden, an die aktualisierte Sicherheitsrichtlinie gebunden zu sein, sobald die Aktualisierungen in Kraft getreten sind.

2.2 Wenn der Lieferant im Voraus über diese Aktualisierungen informiert werden möchte, bevor sie in Kraft treten, kann er sich mit dem auf dieser Webseite zur Sicherheitsrichtlinie bereitgestellten Formular für den Erhalt von Aktualisierungsbenachrichtigungen anmelden. Der Lieferant stellt sicher, dass alle Kontaktinformationen des Lieferanten, die er für das Abonnement der Aktualisierungsmitteilungen angibt, jederzeit aktuell und korrekt sind. Es wird davon ausgegangen, dass der Lieferant eine Aktualisierungsmitteilung erhalten hat, wenn diese per E-Mail versandt wurde, unabhängig davon, ob der Lieferant die Aktualisierungsmitteilung tatsächlich erhält oder nicht.

3. **ZULÄSSIGER ZWECK**.

3.1 **Ausdrückliche Genehmigung**. Der Lieferant darf nur die Amazon-Daten verarbeiten, die im Rahmen des Vertrags ausdrücklich genehmigt wurden, und zwar ausschließlich zum Zweck der Bereitstellung der Produkte und Dienstleistungen im Rahmen des Vertrags (der „zulässige Zweck").

3.2 **Datenaufbewahrung**. Der Lieferant speichert die Amazon-Daten ausschließlich zu dem zulässigen Zweck und so lange, wie es für den zulässigen Zweck erforderlich ist.

3.3 **Ausdrückliche Beschränkungen**. Der Lieferant wird nicht anderweitig: (a) Amazon-Daten verarbeiten, auch nicht in anonymisierter Form; (b) Amazon-Daten, auch nicht in anonymisierter Form, übertragen, vermieten, handeln, tauschen, verkaufen, verleihen, verleasen oder anderweitig verteilen oder Dritten zur Verfügung stellen; oder (c) Modelle der künstlichen Intelligenz (KI) oder des maschinellen Lernens (ML) unter Verwendung von Amazon-Daten entwickeln, trainieren oder verbessern, auch nicht in anonymisierter Form.

4. **MINDESTANFORDERUNGEN AN DIE SICHERHEIT**. Der Lieferant unterhält physische, administrative und technische Sicherheitsvorkehrungen, die mit den Best Practices der Branche übereinstimmen (einschließlich der Standards 27001 und 27002 der International Organization for Standardization („ISO"), dem Cybersecurity Framework des National Institute of Standards and Technology („NIST") oder anderen ähnlichen Standards). Die vom Lieferanten aufrechterhaltenen Sicherheitsvorkehrungen umfassen die unten in den Abschnitten 4.1 bis 4.18 beschriebenen Mindestanforderungen.

4.1 **Schriftliches Informationssicherheitsprogramm**. Der Lieferant muss über ein schriftliches Informationssicherheitsprogramm verfügen, das: (a) geeignete Richtlinien, Verfahren und Standards enthält, die den Anforderungen dieser Sicherheitsrichtlinie entsprechen; (b) einen Ansprechpartner für Sicherheitsfragen benennt, der für die Kommunikation und das Management von Sicherheitsfragen (einschließlich Sicherheitsvorfällen) verantwortlich ist; (c) mindestens einmal jährlich überprüft und bei Bedarf aktualisiert wird; und (d) für das gesamte Personal gilt. Der Lieferant muss sein Informationssicherheitsprogramm überwachen, durchsetzen und Verstöße ahnden.

Die folgende Übersetzung dient nur zu Informationszwecken. Bei Abweichungen und Widersprüchlichkeiten zwischen dieser Übersetzung und der zuletzt aktualisierten englischen Fassung (einschließlich aufgrund von Übersetzungsverzögerungen) hat die englische Fassung Vorrang.

4.2 **Patch-Management**. Der Lieferant muss die abgedeckten Informationssysteme mit den neuesten Upgrades, Updates, Fehlerkorrekturen und neuen Versionen auf dem neuesten Stand halten. Der Lieferant muss Abhilfemaßnahmen für nicht zu patchende Systeme ergreifen.

4.3 **Protokollierung**. Der Lieferant wird Audit-, Ereignis- und Sicherheitsprotokolle erfassen, verwalten und aufbewahren, einschließlich: (a) Protokolldaten über die (autorisierte und unautorisierte) Nutzung von Amazon-Konten oder Zugangsdaten, die dem Lieferanten für einen zulässigen Zweck zur Verfügung gestellt wurden, und (b) Protokolldaten über die Identifizierung oder den Versuch der Identifizierung von Amazon-Personal oder Personal, das Zugriff auf Amazon-Daten oder abgedeckte Informationssysteme hat. Diese Protokolle müssen ausreichende Daten enthalten, um jedes protokollierte Ereignis zu identifizieren: (i) das Personal oder das Konto, das das Ereignis ausgelöst hat, (ii) der Zeitpunkt des Ereignisses und (iii) das System, die Daten oder andere Ressourcen, die betroffen sind. Der Lieferant wird diese Protokolle regelmäßig analysieren, um unautorisierte Aktivitäten zu erkennen, zu untersuchen und zu beheben.

4.4 **Abwehr von Malware**. Der Lieferant wird (a) Anti-Malware-Software oder eine gleichwertige Schutzmaßnahme für alle betroffenen Informationssysteme einsetzen; (b) die Updates, Signaturen und Konfigurationen der Anti-Malware-Software oder einer gleichwertigen Schutzmaßnahme aufrechterhalten; und (c) die Systeme so konfigurieren, dass die Installation, Verbreitung und Ausführung von bösartigem oder nicht autorisiertem Code erkannt, verhindert und behoben wird.

4.5 **Risikomanagementprogramm.** Der Lieferant wird über ein schriftliches Risikomanagementprogramm für die Informationssicherheit verfügen, das Prozesse für die Risikoanalyse, Risikobehandlung, Risikoakzeptanz und Ausnahmen definiert.

4.6 **Schulung zum Sicherheitsbewusstsein**. Der Lieferant verpflichtet sich, das Personal bei der Einstellung und danach mindestens einmal jährlich in den Bereichen Informationssicherheit und Datenschutz zu schulen. Der Lieferant stellt außerdem sicher, dass das Personal rechtzeitig über Aktualisierungen der Sicherheitsrichtlinien und des Datenschutzes des Lieferanten informiert wird.

4.7 **Datenbestand**. Der Lieferant muss Informationen darüber dokumentieren und pflegen, (a) welche Amazon-Daten er verarbeitet und (b) wie und wo diese Amazon-Daten verarbeitet werden (z. B. in einem aktuellen Architekturdiagramm). Auf Anfrage von Amazon hat der Lieferant diese Informationen an Amazon weiterzugeben.

4.8 **Sicherheitstests.**

4.8.1 Der Lieferant muss jährliche Tests durchführen, um sicherzustellen, dass er die Anforderungen dieser Sicherheitsrichtlinie erfüllt.

4.8.2 Der Lieferant muss mindestens einmal jährlich Penetrationstests seiner Sicherheitsvorkehrungen durchführen. Die Penetrationstests müssen Folgendes umfassen: (a) Tests innerhalb und außerhalb des Netzwerks des Lieferanten, (b) Social Engineering (z. B. Phishing-Simulationen), und (c) Sicherheitstests für drahtlose Netzwerke. Der Lieferant muss identifizierte Schwachstellen im Rahmen seines Schwachstellenmanagementprogramms beheben. Auf Anfrage von Amazon muss der Lieferant Amazon die Ergebnisse solcher Penetrationstests und der Behebung von Schwachstellen zur Verfügung stellen.

4.9 **Netzwerksicherheit**. Der Lieferant schützt die abgedeckten Informationssysteme, indem er den unbefugten Netzwerkzugriff, insbesondere von externen Netzwerken, einschränkt. Der Lieferant unterhält und konfiguriert Firewalls oder andere gleichwertige Schutzmaßnahmen zum Schutz der Systeme vor unbefugtem Zugriff und überprüft die Firewall-Regelsätze mindestens einmal jährlich, um sicherzustellen, dass für alle Regeln gültige, dokumentierte Geschäftsfälle vorliegen.

Die folgende Übersetzung dient nur zu Informationszwecken. Bei Abweichungen und Widersprüchlichkeiten zwischen dieser Übersetzung und der zuletzt aktualisierten englischen Fassung (einschließlich aufgrund von Übersetzungsverzögerungen) hat die englische Fassung Vorrang.

4.10 **Geeignete Umgebung**. Der Lieferant wird Amazon-Daten nur in einer Umgebung verarbeiten, die für ihren Zweck geeignet ist, und wird Amazon-Daten nicht in einer Testumgebung verarbeiten, es sei denn, dies ist im Rahmen des Vertrags gestattet.

4.11 **Verschlüsselung**. Der Lieferant wird alle ruhenden Amazon-Daten und alle Daten, die über externe Netzwerke übertragen werden, gemäß den Best Practices der Branche verschlüsseln. Wenn Amazon-Daten über interne Netzwerke des Lieferanten übertragen werden, müssen sie über ein verschlüsseltes Protokoll übertragen werden, das den Best Practices der Branche entspricht. Der Lieferant verwaltet und sichert die Verschlüsselungsschlüssel gemäß den Best Practices der Branche.

4.12 **Kontrollierte Nutzung von Administratorrechten**. Der Lieferant verwaltet die administrativen Funktionen in Übereinstimmung mit dem NIST Cybersecurity Framework oder ISO 27002. Der Lieferant wird zumindest die administrativen Konten von den Standardkonten trennen und die administrativen Konten auf die Fähigkeiten beschränken, die für die Ausführung der administrativen Funktionen erforderlich sind. Der Lieferant protokolliert alle administrativen Kontobewegungen in einer Weise, die einem einzelnen Benutzer zugeordnet werden kann. Die einem Standardkonto zur Verfügung gestellten administrativen Funktionen werden auf der Basis der geringsten Rechte und in einer Weise protokolliert, die einem einzelnen Benutzer zugeordnet werden kann.

4.13 **Zugriffskontrolle.**

4.13.1 **Eindeutige IDs**. Der Lieferant vergibt individuelle, eindeutige IDs an Mitarbeiter mit Zugriff auf Amazon-Daten oder abgedeckte Informationssysteme, einschließlich Konten mit administrativem Zugriff.

4.13.2 „**Need To Know**“**-Basis**. Der Lieferant wird den Zugang zu Amazon-Daten und abgedeckten Informationssystemen nur auf Mitarbeiter beschränken, die für einen zulässigen Zweck unbedingt Zugang zu den Daten benötigen („Need-to-know”).

4.13.3 **Überprüfung des Benutzerzugangs**. Der Lieferant wird mindestens alle 90 Tage die Liste des Personals und der Dienste, die Zugang zu Amazon-Daten und abgedeckten Informationssystemen haben, überprüfen und den Zugang von Konten entfernen, die ihn nicht mehr benötigen.

4.13.4 **Single Sign-On (SSO**). Alle Dienste des Lieferanten, die eine Authentifizierung von Amazon-Mitarbeitern erfordern, müssen mit einem Amazon-Identitätsanbieter (z. B. Amazon Federate) integriert werden, um eine solche Authentifizierung zu ermöglichen. Solche Dienste dürfen keine vom Lieferanten bereitgestellten oder vom Lieferanten verwalteten Anmeldedaten zur Authentifizierung verwenden.

4.14 **Passwortverwaltung.**

4.14.1**Starke Passwörter**. Der Lieferant wird auf den abgedeckten Informationssystemen keine vom Hersteller bereitgestellten Standardwerte für Systempasswörter und andere Sicherheitsparameter verwenden. Der Lieferant wird für alle abgedeckten Informationssysteme die Verwendung von „starken Passwörtern” gemäß den in NIST SP 800-63B beschriebenen Best Practices vorschreiben und sicherstellen. Der Lieferant wird verlangen, dass alle Passwörter und Zugangsdaten vertraulich behandelt und nicht an das Personal weitergegeben werden.

4.14.2 **Sperrung**. Der Lieferant wird eine „Kontosperre” einrichten und durchsetzen, indem er Konten mit Zugang zu Amazon-Daten oder abgedeckten Informationssystemen deaktiviert, wenn ein Konto maximal zehn (10) aufeinanderfolgende falsche Passwortversuche verzeichnet.

4.15 **Fernzugriff; Multi-Faktor-Authentifizierung**. Der Lieferant wird für den Fernzugriff auf ein Netzwerk, ein System, eine Anwendung oder einen anderen Vermögenswert des Lieferanten eine Multi-Faktor-Authentifizierung (d. h. mindestens zwei Faktoren zur Authentifizierung eines Benutzers) einführen.

Die folgende Übersetzung dient nur zu Informationszwecken. Bei Abweichungen und Widersprüchlichkeiten zwischen dieser Übersetzung und der zuletzt aktualisierten englischen Fassung (einschließlich aufgrund von Übersetzungsverzögerungen) hat die englische Fassung Vorrang.

4.16 **„Massenhafter" Zugriff**. Für die Zwecke dieses Abschnitts bedeutet „Massenzugriff" den Zugriff auf Daten mittels Datenbankabfrage, Berichterstellung oder sonstiger Massenübertragung von Daten.

4.16.1 Sofern nicht ausdrücklich in der Vereinbarung oder anderweitig von Amazon schriftlich festgelegt, wird der Lieferant nicht „massenhaft" auf Amazon-Daten zugreifen und den Zugriff auf diese Daten nicht gestatten, unabhängig davon, ob die Amazon-Daten in einer von Amazon oder vom Lieferanten kontrollierten Datenbank oder auf andere Weise gespeichert sind, einschließlich der Speicherung in dateibasierten Archiven (z. B. Flat Files).

4.16.2 Wenn Amazon den „Massen"-Zugriff genehmigt, wird der Lieferant: (a) einen solchen Zugriff nur auf bestimmte Mitarbeiter beschränken, die ihn benötigen, und (b) eine ausdrückliche Genehmigung und Protokollierung eines solchen Zugriffs gemäß den Anforderungen von Abschnitt 4.3 verlangen. Auf Anfrage von Amazon in Koordination mit den Sicherheitsüberprüfungen gemäß Abschnitt 10 oder den Sicherheitsvorfällen gemäß Abschnitt 11 wird der Lieferant Amazon alle in diesem Abschnitt genannten Protokolle über den „Massen"-Zugriff zur Verfügung stellen.

4.17 Datentrennung. Der Lieferant wird die Amazon-Daten jederzeit physisch oder logisch von den Daten des Lieferanten und von denen Dritter trennen. Falls eine Trennung nicht möglich ist, stellt der Lieferant sicher, dass Amazon-Daten zum Zwecke der Protokollierung, Löschung und Reaktion auf Zwischenfälle von anderen Daten unterscheidbar sind.

4.18 **Datenschutz durch das Personal des Lieferanten.**

4.18.1 Der Lieferant trifft alle angemessenen Vorkehrungen, um sicherzustellen, dass das Personal, dem Zugang zu Amazon-Daten gewährt wird, deren Vertraulichkeit wahrt und sie nur für einen erlaubten Zweck verwendet. Diese Vorsichtsmaßnahmen müssen die Auferlegung von Vertraulichkeitsanforderungen durch eine Geheimhaltungsvereinbarung oder eine Richtlinie des Lieferanten beinhalten.

4.18.2 Für alle Mitarbeiter, die (a) keinen Zugang mehr zu Amazon-Daten benötigen oder (b) nicht mehr als Mitarbeiter des Lieferanten gelten, wird der Lieferant den Zugang zu Amazon-Daten und abgedeckten Informationssystemen innerhalb von 24 Stunden beenden. Wenn ein Mitarbeiter mehr als 24 Stunden nach (a) oder (b) weiterhin Zugang zu Amazon-Daten oder abgedeckten Informationssystemen hat, wird der Lieferant Amazon innerhalb von 24 Stunden, nachdem er davon Kenntnis erlangt hat, per E-Mail an security@amazon.com über diesen fortgesetzten Zugang informieren.

5. **ANFORDERUNGEN AN DIE ZAHLUNGSSICHERHEIT**. Wenn der Lieferant Zugang zu den Daten von Zahlungskarteninhabern hat oder diese verarbeiten wird, wird der Lieferant die neueste Version des Payment Card Industry Data Security Standard (PCI DSS) einhalten.

6. **UNTERAUFTRAGNEHMER.**

6.1 Der Lieferant wird ohne die vorherige schriftliche Zustimmung von Amazon keine seiner Verpflichtungen im Rahmen dieser Sicherheitsrichtlinie an Dritte (zusammenfassend „Unterauftragnehmer") weitergeben oder delegieren. Ungeachtet des Bestehens oder der Bedingungen eines Unterauftrags oder einer Weiterdelegierung bleibt der Lieferant für die vollständige Erfüllung seiner Verpflichtungen aus dieser Sicherheitsrichtlinie verantwortlich. Die Bedingungen dieser Sicherheitsrichtlinie sind für die Unterauftragnehmer und das Personal der Unterauftragnehmer des Lieferanten verbindlich.

6.2 Falls der Lieferant von Unterauftragnehmern abgedeckte Informationssysteme einsetzt, wird der Lieferant eine Sicherheitsüberprüfung der von Unterauftragnehmern abgedeckten Informationssysteme und ihrer Schutzmaßnahmen durchführen und Amazon auf Anfrage einen regelmäßigen Bericht über die Schutzmaßnahmen der von Unterauftragnehmern abgedeckten Informationssysteme in dem von Amazon gewünschten Format (z. B. Statement on Standards for Attestation Engagements no. 16 (SSAE 16)) bereitstellen.

Die folgende Übersetzung dient nur zu Informationszwecken. Bei Abweichungen und Widersprüchlichkeiten zwischen dieser Übersetzung und der zuletzt aktualisierten englischen Fassung (einschließlich aufgrund von Übersetzungsverzögerungen) hat die englische Fassung Vorrang.

7. ZUGANG ZU VON AMAZON VERWALTETEN INFORMATIONSSYSTEMEN. Amazon kann dem Lieferanten das Recht einräumen, Amazon-Daten über Webportale oder andere nicht-öffentliche Websites oder Extranets (jeweils ein „von Amazon verwaltetes Informationssystem") ausschließlich zu dem erlaubten Zweck zu verarbeiten. Wenn Amazon dem Lieferanten erlaubt, Amazon-Daten über ein von Amazon verwaltetes Informationssystem zu verarbeiten, müssen der Lieferant und sein Personal die folgenden Anforderungen einhalten:

7.1 **Konten**. Der Lieferant muss sicherstellen, dass das Personal des Lieferanten nur das/die von Amazon für jede Person festgelegte(n) Konto/Konten des von Amazon verwalteten Informationssystems verwendet und das Personal des Lieferanten verpflichtet, seine Zugangsdaten vertraulich zu behandeln und nicht weiterzugeben.

7.2 **Systeme**. Der Lieferant und seine Mitarbeiter werden die von Amazon verwalteten Informationssysteme nur über Computer- oder Verarbeitungssysteme oder -anwendungen nutzen, (a) auf denen vom Lieferanten verwaltete Betriebssysteme laufen und die eine vollständige Festplattenverschlüsselung verwenden, und (b) die die Anforderungen der Abschnitte 4.2 (Patch-Management), 4.4 (Abwehr von Malware) und 4.9 (Netzwerksicherheit) erfüllen.

7.3 **Beschränkungen**. Sofern nicht im Voraus schriftlich von Amazon genehmigt, werden der Lieferant und dessen Personal keine Amazon-Daten aus einem von Amazon verwalteten Informationssystem herunterladen, spiegeln oder dauerhaft auf einem Medium speichern.

7.4 **Kündigung des Kontos**. Für alle Mitarbeiter, die (a) keinen Zugang mehr zum von Amazon verwalteten Informationssystem benötigen oder (b) nicht mehr als Mitarbeiter des Lieferanten gelten (z. B. wenn die betreffende Person aus dem Arbeitsverhältnis mit dem Lieferanten ausscheidet), wird der Lieferant unverzüglich (innerhalb von maximal 24 Stunden) den Zugang dieser Mitarbeiter zum von Amazon verwalteten Informationssystem beenden oder Amazon benachrichtigen, damit dieser Zugang entfernt wird.

8. **AMAZON-DOMAINS ODER -URLS.** Jede Domain oder URL, die der Lieferant für die alleinige Nutzung durch Amazon zur Verfügung stellt, darf vom Lieferanten für mindestens 5 Jahre nach Kündigung der Vereinbarung nicht an Dritte vergeben oder von diesen weiterverwendet werden.

9. RÜCKGABE UND LÖSCHUNG VON DATEN; FORENSISCHE VERNICHTUNG VON DATENTRÄGERN.

9.1 **Datenrückgabe und -löschung**. Auf Aufforderung von Amazon wird der Lieferant alle Amazon-Daten gemäß der Aufforderung von Amazon zur Rückgabe und/oder Löschung unverzüglich (jedoch innerhalb von höchstens 72 Stunden) an Amazon zurückgeben und dauerhaft und sicher löschen. Der Lieferant wird außerdem alle aktiven (online oder über das Netzwerk zugänglichen) Instanzen der Amazon-Daten innerhalb von 30 Tagen nach Beendigung des zulässigen Zwecks oder nach Kündigung oder Ablauf der Vereinbarung, je nachdem, was früher eintritt, dauerhaft und sicher löschen. Auf Verlangen von Amazon wird der Lieferant schriftlich bestätigen, dass alle Amazon-Daten gelöscht worden sind. Zur Klarstellung: Dieser Abschnitt gilt nicht für Archivkopien gemäß Abschnitt 9.3.

9.2 **Datenbereinigung**. Alle vom Lieferanten gelöschten Amazon-Daten werden gemäß den in NIST SP 800-88 Revision 1, Guidelines for Media Sanitization (Dezember 18, 2014, Appendix A) enthaltenen Mindestempfehlungen für die Bereinigung des jeweiligen Gerätetyps gelöscht. Falls in NIST SP 800-88 keine Richtlinien für den entsprechenden Gerätetyp enthalten sind, vernichtet der Lieferant das Gerät, das Amazon-Daten enthält, auf eine der folgenden Arten: (a) Bereinigung gemäß NIST SP 800-88, (b) Vernichtung gemäß NIST SP 800-88 oder (c) gemäß anderen Standards, die Amazon je nach Klassifizierung und Sensibilität der Amazon-Daten verlangt.

9.3 **Archivierungskopien**. Wenn der Lieferant gesetzlich verpflichtet ist, Archivkopien der Amazon-Daten aufzubewahren, wird der Lieferant die archivierten Amazon-Daten nicht für andere Zwecke verwenden und bleibt an alle seine Verpflichtungen gemäß dieser Sicherheitsrichtlinie gebunden. Alle archivierten Amazon-Daten müssen verschlüsselt und an einem Ort gespeichert werden, an dem das abgedeckte Informationssystem, das die verschlüsselten Amazon-Daten beherbergt oder speichert, keinen Zugang zu einer Kopie des/der für die

Die folgende Übersetzung dient nur zu Informationszwecken. Bei Abweichungen und Widersprüchlichkeiten zwischen dieser Übersetzung und der zuletzt aktualisierten englischen Fassung (einschließlich aufgrund von Übersetzungsverzögerungen) hat die englische Fassung Vorrang.

Verschlüsselung verwendeten Schlüssel(s) hat. Jede Offline- oder „kalte" (d. h. nicht zur sofortigen oder interaktiven Nutzung verfügbare) Sicherung muss in einer physisch sicheren Einrichtung aufbewahrt werden.

9.4 **Forensische Vernichtung von Medien**. Vor der Entsorgung von Hardware, Software oder anderen Medien, die Amazon-Daten enthalten oder enthalten haben, führt der Lieferant eine vollständige forensische Vernichtung der Hardware, Software oder anderer Medien gemäß NIST SP 800-88, Anhang A durch. Diese Vernichtungsanforderung gilt nicht für Speichermedien, zu denen der Lieferant keinen physischen Zugang oder über die er keine Kontrolle hat. In solchen Fällen stellt der Lieferant sicher, dass die Amazon-Daten nach den Best Practices der Branche sicher gelöscht werden, wenn sie nicht mehr benötigt werden.

> 9.4.1 Sofern der Lieferant nicht im Voraus eine ausdrückliche schriftliche Genehmigung von Amazon erhält, wird er Hardware, Software oder andere Medien, die zu irgendeinem Zeitpunkt Amazon-Daten enthalten haben, nicht verkaufen, weiterveräußern, verschenken, wiederaufbereiten oder anderweitig weitergeben, es sei denn, die Daten wurden in Übereinstimmung mit diesem Abschnitt forensisch vernichtet.

10. **SICHERHEITSÜBERPRÜFUNGEN**. Auf Anfrage von Amazon wird der Lieferant: (a) eine Amazon-Risikobewertung durchführen, (b) von Amazon angeforderte Nachweise zur Verfügung stellen, um die Einhaltung dieser Sicherheitsrichtlinien durch den Lieferanten zu bestätigen, (c) Amazon oder einem von Amazon beauftragten Dritten gestatten, eine Überprüfung der Einhaltung dieser Sicherheitsrichtlinien durch den Lieferanten vorzunehmen und/oder (d) Amazon alle in Abschnitt 4.3 genannten Protokolle im Format des Open Cybersecurity Schema Framework (OCSF) zur Verfügung stellen. Wenn der Lieferant verlangt, dass die Nachweise persönlich oder im Rahmen einer Vor-Ort-Inspektion überprüft werden, anstatt sie Amazon per Fernzugriff zur Überprüfung zur Verfügung zu stellen, trägt der Lieferant die Kosten für die Reise und andere Ausgaben im Zusammenhang mit einer solchen Vor-Ort-Inspektion. Werden bei einer Bewertung oder Überprüfung Feststellungen getroffen, ergreift der Lieferant auf eigene Kosten unverzüglich alle angemessenen Maßnahmen, um diese Feststellungen zur angemessenen Zufriedenheit von Amazon und innerhalb eines vereinbarten Zeitrahmens zu beheben.

11. **SICHERHEITSVORFÄLLE.**

11.1 **Benachrichtigung über Sicherheitsvorfälle**. Der Lieferant wird Amazon so schnell wie möglich benachrichtigen, spätestens jedoch innerhalb von 24 Stunden, nachdem der Lieferant weiß oder vernünftigerweise davon ausgeht, dass es zu einem unbefugten Zugriff, einer unbefugten Erfassung, einem unbefugten Erwerb, einer unbefugten Nutzung, einer unbefugten Übertragung, einer unbefugten Offenlegung, einer unbefugten Beschädigung oder einem unbefugten Verlust von Amazon-Daten oder eines abgedeckten Informationssystems gekommen ist (ein „Sicherheitsvorfall"). Der Lieferant sendet die Benachrichtigungen über Sicherheitsvorfälle an security@amazon.com.

11.2 **Plan zur Reaktion auf Sicherheitsvorfälle**. Der Lieferant unterhält einen schriftlichen Plan zur Reaktion auf Sicherheitsvorfälle und stellt Amazon auf Anfrage eine Kopie davon zur Verfügung. Der Lieferant behebt jeden Sicherheitsvorfall zeitnah gemäß dem schriftlichen Reaktionsplan des Lieferanten und den Best Practices der Branche. Der Lieferant wird den Plan mindestens einmal jährlich überprüfen, testen und (falls erforderlich) aktualisieren.

11.3 **Zusammenarbeit mit Amazon**. Der Lieferant wird (a) Amazon bei der Untersuchung des Sicherheitsvorfalls unterstützen; (b) Interviews mit dem Personal und anderen Personen, die an dem Sicherheitsvorfall oder der Reaktion darauf beteiligt waren, ermöglichen; (c) schriftliche Details über die Untersuchung des Sicherheitsvorfalls und die Reaktion des Lieferanten aufbewahren, und (d) Amazon alle relevanten Aufzeichnungen, Protokolle, Dateien, Datenberichte, forensische Berichte, Untersuchungsberichte und andere von Amazon angeforderte Materialien zur Verfügung stellen.

Die folgende Übersetzung dient nur zu Informationszwecken. Bei Abweichungen und Widersprüchlichkeiten zwischen dieser Übersetzung und der zuletzt aktualisierten englischen Fassung (einschließlich aufgrund von Übersetzungsverzögerungen) hat die englische Fassung Vorrang.

11.4 **Benachrichtigung Dritter**. Soweit gesetzlich nicht anders vorgeschrieben, holt der Lieferant die vorherige schriftliche Zustimmung von Amazon ein, bevor er: (a) Dritte (einschließlich Aufsichtsbehörden oder Kunden) über einen Sicherheitsvorfall benachrichtigt; oder (b) Amazon in einer Benachrichtigung oder öffentlichen Erklärung über einen Sicherheitsvorfall nennt. Sofern gesetzlich nicht anders vorgeschrieben, hat Amazon das Recht, zu bestimmen, ob Dritte über einen Sicherheitsvorfall benachrichtigt werden sollen und in welcher Form, zu welchem Zeitpunkt und mit welchem Inhalt dies geschehen soll.

12. **Benachrichtigung über rechtliche Schritte**. Benachrichtigung über rechtliche Schritte. Sofern dies nicht gesetzlich verboten ist, wird der Lieferant Amazon ausreichende Informationen zur Verfügung stellen, um Amazon in die Lage zu versetzen, eine einstweilige Verfügung oder ein anderes geeignetes Rechtsmittel zu erwirken, wenn Amazon-Daten als Reaktion auf ein Gerichtsverfahren oder ein anderes anwendbares Gesetz angefordert werden.

13. **DEFINITIONEN**.

13.1 „**Vereinbarung**" bezeichnet jede Vereinbarung, die auf diese Sicherheitsrichtlinie verweist.

13.2 „**Amazon**" bezeichnet Amazon.com, Inc. und die mit ihr verbundenen Unternehmen.

13.3 „**Amazon-Daten**" bezeichnet: (a) alle vertraulichen Amazon-Daten (wie in anderen Vereinbarungen zwischen den Parteien definiert); (b) alle Daten, Aufzeichnungen, Dateien, Inhalte oder Informationen in jeglicher Form, die der Lieferant oder seine verbundenen Unternehmen von oder im Namen von Amazon oder anderweitig im Zusammenhang mit der Vereinbarung erworben, abgerufen, gesammelt, erhalten, gespeichert oder aufbewahrt haben; und (c) aus (a) oder (b) abgeleitete Informationen, auch wenn diese anonymisiert sind.

13.4 „**Anonymisieren**" bezeichnet die Verarbeitung von Daten oder Informationen (einschließlich Amazon-Daten) auf eine Art und Weise oder in einer Form, die eine Identifizierung nicht zulässt und die nicht Amazon oder einem Nutzer, einer Gerätekennung, einer Quelle, einem Produkt, einer Dienstleistung, einem Kontext oder einer Marke zuzuordnen ist.

13.5 „**Abgedeckte Informationssysteme**" bezeichnet alle Systeme, die der Lieferant zur Verarbeitung von Amazon-Daten verwendet.

13.6 „**Personal**" bezeichnet die Mitarbeiter des Lieferanten oder Unterauftragnehmers, Vertreter, Unterauftragnehmer und andere autorisierte Nutzer seiner Systeme und Netzwerkressourcen.

13.7 „**Verarbeiten**" bezeichnet die Durchführung von Vorgängen an Daten, wie z. B. Zugriff, Nutzung, Sammlung, Empfang, Speicherung, Veränderung, Übertragung, Verbreitung oder anderweitige Bereitstellung, Löschung oder Vernichtung.

13.8 „**Lieferant**" bezeichnet jeden in einem Vertrag definierten Lieferanten, Verkäufer oder Auftragnehmer und jeden anderen Anbieter, der einem Vertrag unterliegt.