Die nachstehende Übersetzung wird nur zu Informationszwecken bereitgestellt. Im Falle von Unstimmigkeiten, Widersprüchen oder Konflikten zwischen dieser Übersetzung und der englischen Version (insbesondere aufgrund von Verzögerungen bei der Übersetzung) ist die englische Version maßgebend.

SICHERHEITSRICHTLINIE FÜR ANBIETER

Zuletzt aktualisiert am 28. Januar 2022

1. UMFANG; DEFINITIONEN.

1.1 Sicherheitsrichtlinie. Der Lieferant hält in jeder Hinsicht die in dieser Richtlinie dargelegten Anforderungen von Amazon an die Informationssicherheit (die „**Sicherheitsrichtlinie**“) ein. Diese Sicherheitsrichtlinie gilt für die Leistung des Lieferanten im Rahmen der Vereinbarung und für jeden Zugriff und jede Erfassung, Nutzung, Speicherung, Übertragung, Offenlegung, Vernichtung oder Löschung von Amazon-Informationen durch den Lieferanten sowie für Sicherheitsvorfälle in Bezug auf diese Informationen. Diese Sicherheitsrichtlinie beschränkt keine anderen Verpflichtungen des Lieferanten, einschließlich anderer Vereinbarungen mit Amazon oder anderer Gesetze, die für den Lieferanten gelten, der Leistung des Lieferanten im Rahmen anderer Vereinbarungen mit Amazon, der Amazon-Informationen oder des zulässigen Zwecks. Sollte diese Sicherheitsrichtlinie im Widerspruch zu einer Geheimhaltungsvereinbarung zwischen den Parteien oder einer anderen Vereinbarung, die für die Parteien gilt, stehen, so wird der Lieferant Amazon unverzüglich darüber informieren und die Anforderungen erfüllen, die den Schutz der Amazon-Informationen stärker gewährleisten, es sei denn, die weniger schützenden Anforderungen haben ausdrücklich Vorrang vor den stärker schützenden Anforderungen (was von Amazon festgelegt werden kann). Amazon kann diese Sicherheitsrichtlinie von Zeit zu Zeit nach eigenem Ermessen ändern, vorausgesetzt, dass, wenn solche Änderungen wirtschaftlich nicht angemessen sind, Amazon auf Anfrage angemessene zusätzliche Gebühren vereinbaren wird.

1.2 Definitionen.

1.2.1 „**Aggregieren**“ bedeutet, Amazon-Informationen mit Daten oder Informationen des Lieferanten oder eines Dritten zu kombinieren oder zu speichern.

1.2.2 „**Vereinbarung**“ bedeutet jede Vereinbarung, die auf diese Sicherheitsrichtlinie verweist.

1.2.3 „**Amazon**“ bedeutet Amazon.com, Inc. und seine verbundene Unternehmen.

1.2.4 „**Anonymisieren**“ bedeutet, Daten oder Informationen (einschließlich Amazon-Informationen) auf eine Art und Weise oder in einer Form zu verwenden, zu erfassen, zu speichern, zu übertragen oder zu verändern, die keine Identifizierung von Amazon oder einem Benutzer, einer Gerätekennung, einer Quelle, einem Produkt, einer Dienstleistung, einem Kontext oder einer Marke davon darstellt, ermöglicht oder anderweitig darauf zurückzuführen ist.

1.2.5 „**Amazon-Informationen**“ bedeutet einzeln und zusammengenommen: (a) alle vertraulichen Informationen von Amazon (wie in einer Geheimhaltungsvereinbarung oder einer anderen Vereinbarung zwischen den Parteien definiert); (b) alle anderen Daten, Aufzeichnungen, Dateien, Inhalte oder Informationen in jeder Form und jedem Format, die vom Lieferanten oder seinen verbundenen Unternehmen von oder im Namen von Amazon oder anderweitig in Verbindung mit dieser Sicherheitsrichtlinie oder den Dienstleistungen oder zur Erfüllung oder Ausübung von Rechten der Parteien im Rahmen oder in Verbindung mit der Vereinbarung erworben, abgerufen, gesammelt, erhalten, gespeichert oder aufbewahrt werden; und (c) Informationen, die aus (a) oder (b) abgeleitet werden, auch wenn sie anonymisiert sind.

1.2.6 „Lieferant“ bezeichnet jeden Lieferanten, Anbieter oder Auftragnehmer, der in einer Vereinbarung definiert ist, und jeden anderen an eine Vereinbarung gebundenen Dienstleister.

1.3 Zulässiger Zweck. Der Lieferant darf nur auf die Amazon-Informationen zugreifen und diese erfassen, verwenden, speichern und übertragen, die ausdrücklich gemäß der Vereinbarung und ausschließlich zum Zwecke der Bereitstellung der Produkte oder Dienstleistungen im Rahmen der Vereinbarung, im Einklang mit den Lizenzen (falls vorhanden), die gemäß dieser Sicherheitsrichtlinie gewährt werden, genehmigt wurden (der „**zulässige Zweck**“). Sofern nicht ausdrücklich im Rahmen der Vereinbarung genehmigt, wird der Lieferant keine Amazon-Informationen abrufen, erfassen, verwenden, speichern oder übertragen und keine Amazon-Informationen zusammenfassen, auch nicht in anonymisierter Form. Außer mit der vorherigen ausdrücklichen schriftlichen Zustimmung von Amazon wird der Lieferant (a) keine Amazon-Informationen übertragen, vermieten, tauschen, handeln, verkaufen, verleihen oder verleasen oder anderweitig verteilen oder Dritten zugänglich machen oder (b) Amazon-Informationen mit anderen Informationen oder Daten zusammenfassen, selbst wenn sie anonymisiert sind.

2. SICHERHEITSRICHTLINIE VON AMAZON.

2.1 Grundlegende Anforderungen an die Sicherheit. Der Lieferant trifft im Einklang mit den aktuell besten Branchenstandards und solchen anderen Anforderungen, die von Amazon auf der Grundlage der Klassifizierung und Sensibilität der Amazon-Informationen festgelegten Anforderungen physische, administrative und technische Sicherheitsvorkehrungen und andere Sicherheitsmaßnahmen, um (a) die Sicherheit und Vertraulichkeit der abgerufenen, erfassten, verwendeten, gespeicherten oder vom Lieferanten übermittelten Amazon-Informationen zu wahren, und (b) diese Informationen vor bekannten oder vernünftigerweise erwarteten Bedrohungen oder Gefahren für ihre Sicherheit und Integrität, versehentlichem Verlust, Veränderung und Offenlegung sowie vor allen anderen unrechtmäßigen Formen der Verarbeitung zu schützen. Der Lieferant erfüllt ohne Einschränkung die folgenden Anforderungen für alle Systeme, die der Lieferant zur Verarbeitung von Amazon-Informationen verwendet oder die Zugriff auf Amazon-Informationen haben (die „**Amazon-Informationssysteme**“):

2.1.1 Netzwerksicherheit. Der Lieferant schützt alle Amazon-Informationssysteme, indem er den unbefugten Netzwerkzugriff, insbesondere aus dem externen Internet, einschränkt. Der Lieferant installiert und pflegt eine effektive Netzwerksicherheitslösung, wie z. B. eine Firewall, um die Amazon-Informationen jederzeit zu schützen.

2.1.2 Updates. Wie in der Special Publication („SP“) 800-40 Revision 3 des National Institute of Standards and Technology („NIST“) beschrieben, hält der Lieferant die Amazon-Informationssysteme mit den neuesten Upgrades, Updates, Bugfixes und neuen Versionen und mit allen anderen Änderungen, die zur Gewährleistung der Sicherheit der Amazon-Informationen erforderlich sind, auf dem neuesten Stand.

2.1.3 Anti-Malware. Der Lieferant setzt jederzeit Anti-Malware-Software oder eine gleichwertige Sicherheitskontrolle ein, um das Risiko einer Gefährdung und Verbreitung von Malware zu mindern. In diesem Fall hält der Lieferant die Anti-Malware-Software auf dem neuesten Stand.

2.1.4 Verschlüsselung. Der Lieferant verschlüsselt Daten im Ruhezustand und Daten, die über offene Netzwerke gesendet werden, in Übereinstimmung mit den bewährten Praktiken der Branche verschlüsseln.

2.1.5 Tests. Der Lieferant testet seine Sicherheitssysteme und -prozesse regelmäßig, um sicherzustellen, dass sie die Anforderungen dieser Sicherheitsrichtlinie oder der zuletzt zwischen dem Lieferanten und Amazon vereinbarten Sicherheitsrichtlinie erfüllen. Soweit es Änderungen an der Sicherheitsrichtlinie gemäß Abschnitt 1.1 gibt, werden diese Änderungen für die Zwecke dieses Abschnitts erst nach Vereinbarung zwischen dem Lieferanten und Amazon wirksam (E-Mail genügt).

2.1.6 Zugangskontrollen. Der Lieferant sichert die Amazon-Informationen unter anderem durch Einhaltung der folgenden Anforderungen:

2.1.6.1 Der Lieferant weist jeder Person mit Computerzugriff auf Amazon-Informationen oder Amazon-Informationssysteme eine eindeutige ID zu.

2.1.6.2 Der Lieferant beschränkt den Zugriff auf Amazon-Informationen auf die Personen, die diese Informationen für einen zulässigen Zweck benötigen („Need-to-know“-Basis).

2.1.6.3 Der Lieferant überprüft regelmäßig die Liste der Personen und Dienste mit Zugriff auf Amazon-Informationen und entfernt Konten, die keinen Zugriff auf Amazon-Informationssysteme mehr benötigen. Diese Überprüfung muss mindestens einmal alle 90 Tage durchgeführt werden.

2.1.6.4 Der Lieferant verwendet keine vom Hersteller vorgegebenen Standardwerte für Systempasswörter und andere Sicherheitsparameter auf Amazon-Informationssystemen. Der Lieferant schreibt die Verwendung von systemerzwungenen „starken Passwörtern" in Übereinstimmung mit den in NIST SP 800-63B beschriebenen bewährten Verfahren auf allen Amazon-Informationssystemen vor und sorgt für die Befolgung. Der Lieferant verlangt, dass alle Passwörter und Zugangsdaten vertraulich behandelt und nicht an Mitarbeiter weitergegeben werden.

2.1.6.5 Der Lieferant behält die „Kontosperre" bei und setzt sie durch, indem er Konten mit Zugriff auf Amazon-Informationen oder Amazon-Informationssysteme deaktiviert, wenn auf einem Konto mehr als zehn (10) aufeinanderfolgende falsche Passwortversuche unternommen werden.

2.1.6.6 Sofern nicht ausdrücklich von Amazon schriftlich genehmigt, trennt der Lieferant die Amazon-Informationen physisch oder logisch jederzeit (einschließlich bei Speicherung, Verarbeitung oder Übertragung) von den Informationen des Lieferanten und Dritter.

2.1.6.7 Wenn Amazon schriftlich zusätzliche physische Zugangskontrollen verlangt, führt der Lieferant diese sicheren physischen Zugangskontrollmaßnahmen ein.

2.1.6.8 Der Lieferant übergibt Amazon auf dessen zumutbare Aufforderung hin (a) Protokolldaten über die gesamte Nutzung (sowohl autorisierte als auch unbefugte) der Amazon-Konten oder Anmeldeinformationen, die dem Lieferanten für einen zulässigen Zweck (z. B. Zugangsdaten für soziale Medien) zur Verfügung gestellt werden, und (b) detaillierte Protokolldaten über das Ausgeben Dritter als Amazon-Mitarbeiter oder Mitarbeiter des Lieferanten, die Zugriff auf Amazon-Informationen haben, oder den Versuch Dritter, sich als solche Mitarbeiter auszugeben.

2.1.6.9 Der Lieferant überprüft die Zugangsprotokolle regelmäßig auf Anzeichen von böswilligem Verhalten oder unbefugtem Zugriff.

2.1.7 Richtlinien des Lieferanten. Der Lieferant wird Richtlinien zur Informations- und Netzwerksicherheit für Mitarbeiter, Unterauftragnehmer, Vertreter und Anbieter führen und durchsetzen, die den in dieser Sicherheitsrichtlinie festgelegten Standards entspricht, einschließlich Methoden zur Erkennung und Protokollierung von Richtlinienverstößen. Auf Anfrage von Amazon wird der Lieferant Amazon-Informationen zu Verstößen gegen die Richtlinien zur Informations- und Netzwerksicherheit des Lieferanten zur Verfügung stellen, wenn entweder der Lieferant oder Amazon den begründeten Verdacht hat, dass ein Sicherheitsvorfall (wie unten definiert) eingetreten sein könnte.

2.1.8 Unteraufträge. Der Lieferant darf ohne vorherige schriftliche Zustimmung von Amazon keine seiner Verpflichtungen gemäß dieser Sicherheitsrichtlinie an Subunternehmer oder Beauftragte (zusammen „**Unterauftragnehmer**") vergeben oder weiterdelegieren. 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 Mitarbeiter des Lieferanten verbindlich. Der Lieferant wird (a) sicherstellen, dass seine Unterauftragnehmer und Mitarbeiter diese Sicherheitsrichtlinie einhalten, und (b) für alle Handlungen, Unterlassungen sowie für Fahrlässigkeit und Fehlverhalten der Unterauftragnehmer und Mitarbeiter des Lieferanten einstehen.

2.1.9 Fernzugriff. Der Lieferant stellt sicher, dass jeder Zugriff auf Amazon-Informationssysteme eine Multi-Faktor-Authentifizierung erfordert (z. B. mindestens zwei separate Faktoren zur Identifizierung von Benutzern erfordert).

2.1.10 Massenzugriff. Für die Zwecke dieses Abschnitts bedeutet „Massenzugriff" den Zugriff auf Daten mittels Datenbankabfrage, Berichterstellung oder sonstiger Massenübertragung von Daten. Sofern nicht ausdrücklich von Amazon schriftlich genehmigt, führt der Lieferant keinen Massenzugriff auf Amazon-Informationen durch und erlaubt keinen derartigen Zugriff, unabhängig davon, ob sich die Amazon-Informationen in einer vom Lieferanten oder von Amazon kontrollierten Datenbank befinden oder auf andere Weise gespeichert sind, einschließlich der Speicherung in dateibasierten Archiven (z. B. Flat Files, usw.). Insbesondere verbietet dieser Abschnitt jeden Zugriff auf Amazon-Informationen, außer den Zugriff

auf einzelne Datensätze, soweit dies für den zulässigen Zweck erforderlich ist. Der Lieferant bewahrt detaillierte Protokolldaten über versuchten oder erfolgreichen Massenzugriff auf Amazon-Informationen auf und legt im Rahmen seiner Verpflichtungen aus Abschnitt 2.5 (Sicherheitsüberprüfung) Berichte aus diesen Protokollen vor. Wenn Amazon dem Lieferanten eine schriftliche Genehmigung für den Massenzugriff auf Amazon-Informationen erteilt, wird der Lieferant (a) diesen Zugriff nur auf bestimmte Mitarbeiter beschränken, die diese Informationen wissen müssen („Need-to-know"-Basis) und (b) Tools verwenden, die den Zugriff einschränken und eine ausdrückliche Autorisierung und Protokollierung aller Zugriffe erfordern.

2.1.11 Mitarbeiter des Lieferanten. Amazon kann den Zugriff von Mitarbeitern des Lieferanten auf Amazon-Informationen davon abhängig machen, dass diese Mitarbeiter individuelle Geheimhaltungsvereinbarungen, deren Form von Amazon vorgegeben wird, unterzeichnen und an Amazon übergeben. Die Mitarbeiter des Lieferanten unterzeichnen die individuellen Geheimhaltungsvereinbarungen, wenn Amazon dies verlangt. Der Lieferant wird von seinen Mitarbeitern, die Zugriff auf die Amazon-Informationen haben (vor der Gewährung des Zugriffs oder der Bereitstellung von Informationen an seine Mitarbeiter), unterzeichnete individuelle Geheimhaltungsvereinbarungen einholen und an Amazon weitergeben. Der Lieferant führt auch eine Liste aller seiner Mitarbeiter, die über Amazon-Informationssysteme auf die Amazon-Informationen zugegriffen oder diese erhalten haben, und stellt diese Liste Amazon auf Verlangen unverzüglich zur Verfügung. Für Mitarbeiter des Lieferanten, die (a) keinen Zugriff mehr auf Amazon-Informationen 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 den Zugriff auf Amazon-Informationen und Amazon-Informationssysteme unverzüglich (innerhalb von maximal 24 Stunden) beenden. Wenn solche Mitarbeiter berechtigt sind, über Amazon-Informationssysteme auf Amazon-Informationen zuzugreifen, wird der Lieferant Amazon ebenfalls innerhalb von 24 Stunden benachrichtigen.

2.2 Zugriff auf das Amazon-Extranet und Lieferantenportale. Amazon kann dem Lieferanten den Zugriff auf Amazon-Informationen über Webportale oder andere nicht öffentliche Websites oder Extranet-Dienste auf der Website oder dem System von Amazon oder Dritten (jeweils ein „**Extranet**") für den zulässigen Zweck gewähren. Wenn Amazon dem Lieferanten den Zugriff auf Amazon-Informationen über ein Extranet gestattet, muss der Lieferant die folgenden Anforderungen erfüllen:

2.2.1 Zulässiger Zweck. Der Lieferant und die Mitarbeiter des Lieferanten werden ausschließlich für den zulässigen Zweck auf das Extranet zugreifen und Amazon-Informationen aus dem Extranet abrufen, sammeln, verwenden, anzeigen, herunterladen oder speichern.

2.2.2 Konten. Der Lieferant trägt dafür Sorge, dass seine Mitarbeiter nur die Extranet-Konten verwenden, die Amazon für die jeweilige Person bestimmt hat, und verpflichtet seine Mitarbeiter, die Zugangsdaten vertraulich zu behandeln.

2.2.3 Systeme. Der Lieferant wird nur über Computer- oder Verarbeitungssysteme oder Anwendungen auf das Extranet zugreifen, auf denen Betriebssysteme laufen, die vom Lieferanten verwaltet werden, und die Folgendes umfassen: (a) Systemnetzwerk-Firewalls gemäß Abschnitt 2.1.1 (Netzwerksicherheit); (b) zentralisierte Patch-Verwaltung gemäß Abschnitt 2.1.2 (Updates); (c) betriebssystemgerechte Anti-Malware-Software gemäß Abschnitt 2.1.3 (Anti-Malware); und (d) vollständige Festplattenverschlüsselung für tragbare Geräte.

2.2.4 Beschränkungen. Sofern nicht im Voraus schriftlich von Amazon genehmigt, darf der Lieferant keine Amazon-Informationen von einem Extranet auf ein Medium herunterladen, spiegeln oder dauerhaft speichern, einschließlich aller Maschinen, Geräte oder Server.

2.2.5 Kontokündigung. Der Lieferant kündigt das Konto eines seiner Mitarbeiter, der berechtigt ist, auf ein Extranet zuzugreifen, kündigen und benachrichtigt Amazon spätestens 24 Stunden danach, wenn dieser Mitarbeiter: (a) keinen Zugriff auf Amazon-Informationen mehr benötigt oder (b) nicht mehr als Mitarbeiter des Lieferanten gilt (z. B. wenn die betreffende Person aus dem Arbeitsverhältnis mit dem Lieferanten ausscheidet).

2.2.6 Systeme Dritter.

2.2.6.1 Der Lieferant wird Amazon im Voraus benachrichtigen und die vorherige schriftliche Genehmigung von Amazon einholen, bevor er ein Drittsystem nutzt, das Amazon-Informationen speichert oder anderweitig Zugriff auf diese Informationen hat, es sei denn, (a) die Daten sind gemäß dieser Sicherheitsrichtlinie verschlüsselt und (b) das Drittsystem hat keinen Zugriff auf den Entschlüsselungscode oder unverschlüsselte Klartextversionen der Daten. Amazon behält sich das Recht vor, vor der Genehmigung eine Amazon-Sicherheitsüberprüfung (gemäß Abschnitt 2.5 (Sicherheitsüberprüfung) des Drittsystems zu verlangen.

2.2.6.2 Nutzt der Lieferant Drittsysteme, die unverschlüsselte Amazon-Informationen speichern oder anderweitig auf unverschlüsselte Amazon-Informationen zugreifen können, so führt der Lieferant eine Sicherheitsüberprüfung der Drittsysteme und ihrer Sicherheitskontrollen durch und stellt Amazon regelmäßige Berichte über die Sicherheitskontrollen des Drittsystems in dem von Amazon angeforderten Format zur Verfügung (z. B. SAS 70 oder seinen Nachfolgerbericht oder einen anderen von Amazon genehmigten anerkannten Industriestandardbericht).

2.3 Aufbewahrung und Vernichtung von Daten.

2.3.1 Aufbewahrung. Der Lieferant bewahrt die Amazon-Informationen nur für den zulässigen Zweck und nur so lange, wie es dafür erforderlich ist, auf.

2.3.2 Rückgabe oder Löschung. Auf Verlangen von Amazon gibt der Lieferant alle Amazon-Informationen unverzüglich (in jedem Fall aber innerhalb von 72 Stunden) an Amazon zurück bzw. löscht sie dauerhaft und sicher gemäß der Mitteilung von Amazon über die erforderliche Rückgabe und/oder Löschung. Der Lieferant löscht außerdem alle live verfügbaren (online oder über das Netzwerk zugänglichen) Instanzen der Amazon-Informationen innerhalb von 30 Tagen nach Abschluss des zulässigen Zwecks oder Kündigung bzw. Ablauf dieser Sicherheitsrichtlinie dauerhaft und sicher. Auf Verlangen von Amazon bestätigt der Lieferant schriftlich, dass alle Amazon-Informationen vernichtet wurden. Zur Klarstellung: Dieser Abschnitt gilt nicht für Archivkopien gemäß Abschnitt 2.3.3.

2.3.3 Archivkopien. Sollte der Lieferant gesetzlich verpflichtet sein, Archivkopien von Amazon-Informationen für steuerliche oder ähnliche behördliche Zwecke aufzubewahren, so müssen diese archivierten Amazon-Informationen auf eine der folgenden Arten gespeichert werden:

2.3.3.1 als „kaltes“ oder Offline-Backup (d. h. nicht zur sofortigen oder interaktiven Verwendung verfügbar), das in einer physisch sicheren Einrichtung aufbewahrt wird, oder

2.3.3.2 verschlüsselt, wobei das System, das die verschlüsselte(n) Datei(en) hostet oder speichert, keinen Zugriff auf eine Kopie des Codes hat, der zur Verschlüsselung verwendet werden.

2.3.4 Wiederherstellung. Führt der Lieferant zum Zwecke der Notfallwiederherstellung eine „Wiederherstellung“ durch (d. h. Zurückgreifen auf ein Backup), so sorgt der Lieferant durch einen entsprechend eingerichteten Prozess dafür, dass alle Amazon-Informationen, die gemäß der Vereinbarung oder dieser Sicherheitsrichtlinie oder einer anderen Vereinbarung mit Amazon gelöscht werden müssen, innerhalb von 24 Stunden nach der Wiederherstellung gemäß diesem Abschnitt 2.3 erneut aus den wiederhergestellten Daten gelöscht oder überschrieben werden. Wenn der Lieferant eine Wiederherstellung für irgendeinen Zweck durchführt, dürfen ohne vorherige schriftliche Genehmigung von Amazon keine Amazon-Informationen auf ein System oder Netzwerk eines Dritten wiederhergestellt werden. Amazon behält sich das Recht vor, eine Amazon-Sicherheitsüberprüfung (gemäß Abschnitt 2.5 (Sicherheitsüberprüfung) des Systems oder Netzwerks des Dritten zu verlangen, bevor die Wiederherstellung von Amazon-Informationen in einem System oder Netzwerk Dritter gestattet wird.

2.3.5 Standards für die Datenbereinigung. Alle vom Lieferanten gelöschten Amazon-Informationen werden in Übereinstimmung mit den Empfehlungen zur minimalen Datenbereinigung, die in NIST SP 800-88 Revision 1, Guidelines for Media Sanitation, 18. Dezember 2014 (verfügbar unter http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), Anhang A, enthalten sind, für die Bereinigung des entsprechenden Gerätetyps gelöscht. In Ermangelung relevanter Leitlinien in NIST SP 800-88, Anhang A, muss das Gerät, das Amazon-Informationen enthält, auf eine der folgenden Arten vernichtet werden: (a) durch Entmagnetisierung magnetischer Medien in einem elektromagnetischen Flussfeld von über 10.000 Gauß, (b) durch Schreddern oder mechanische Zerkleinerung, die zu Partikeln

führt, die kleiner als 2 x 2 mm sind, oder (c) durch andere Standards, die Amazon je nach Klassifizierung und Sensibilität der Amazon-Informationen verlangen kann.

2.4 Forensische Vernichtung. Vor der Entsorgung (gleich auf welche Weise) von Hardware, Software oder anderen Medien, die Amazon-Informationen enthalten oder zu irgendeinem Zeitpunkt enthalten haben, führt der Lieferant eine vollständige forensische Vernichtung der Hardware, Software oder anderer Medien durch, sodass der Abruf der Amazon-Informationen in irgendeiner Form unmöglich ist. Der Lieferant führt die forensische Vernichtung in Übereinstimmung mit den Empfehlungen zur minimalen Datenbereinigung durch, die in NIST SP 800-88, Anhang A, für die Vernichtung des betreffenden Gerätetyps enthalten sind.

2.4.1 Der Lieferant darf keine Hardware, Software oder andere Medien, die Amazon-Informationen enthalten und nicht gemäß diesem Abschnitt 2.4 forensisch vernichtet wurden, verkaufen, weiterverkaufen, spenden, aufarbeiten oder anderweitig übertragen (einschließlich des Verkaufs oder der Übertragung solcher Hardware, Software oder anderer Medien, einer Veräußerung in Verbindung mit einer Liquidation des Unternehmens des Lieferanten oder einer sonstigen Veräußerung).

2.5 Sicherheitsüberprüfung.

2.5.1 Amazon behält sich das Recht vor, den Lieferanten regelmäßig zur Teilnahme an einer Amazon-Risikobewertung anzuhalten.

2.5.2 Zertifizierung. Auf schriftliche Anfrage von Amazon wird der Lieferant Amazon schriftlich bestätigen, dass die im Rahmen der Risikobewertung bereitgestellten Informationen mit dieser zuletzt zwischen dem Lieferanten und Amazon vereinbarten Sicherheitsrichtlinie übereinstimmen. Soweit es Änderungen an der Sicherheitsrichtlinie gemäß Abschnitt 1.1 gibt, werden diese Änderungen für die Zwecke dieses Abschnitts erst nach Vereinbarung zwischen dem Lieferanten und Amazon wirksam (E-Mail genügt).

2.5.3 Weitere Überprüfungen. Amazon behält sich das Recht vor, die Sicherheit von Amazon-Informationssystemen regelmäßig zu überprüfen, jedoch nicht mehr als einmal jährlich, es sei denn, (a) ein früherer erheblicher Mangel wurde innerhalb des Kalenderjahres festgestellt oder (b) Amazon ist von einer Regierungsbehörde oder einer anderen Aufsichtsbehörde verpflichtet, eine solche Überprüfung durchzuführen. Der Lieferant kooperiert und stellt Amazon alle erforderlichen Informationen innerhalb eines angemessenen Zeitrahmens, jedoch nicht länger als 20 Kalendertage ab dem Datum der Anfrage von Amazon zur Verfügung.

2.5.4 Mängelbeseitigung. Werden bei einer Sicherheitsprüfung Mängel identifiziert, so wird der Lieferant auf alleinige Kosten alle angemessenen Maßnahmen ergreifen, um diese Mängel innerhalb eines vereinbarten Zeitrahmens zu beheben.

2.6 Sicherheitsvorfälle.

2.6.1 Der Lieferant informiert Amazon so schnell wie möglich, spätestens jedoch 24 Stunden nach Kenntnisnahme eines tatsächlichen oder vermuteten unbefugten Zugriffs, einer tatsächlichen oder vermuteten Sammlung, Übernahme, Nutzung, Übertragung, Offenlegung, Korruption oder eines Verlusts von Amazon-Informationen oder der Verletzung von Amazon-Informationssystemen (ein „**Sicherheitsvorfall**“). Der Lieferant behebt jeden Sicherheitsvorfall rechtzeitig und lässt Amazon schriftliche Details zur internen Untersuchung des Lieferanten in Bezug auf den Sicherheitsvorfall zukommen. Wenn dies nach geltendem Recht zulässig ist, verpflichtet sich der Lieferant, keine Aufsichtsbehörde oder Kunden im Namen von Amazon zu benachrichtigen, es sei denn, Amazon verlangt ausdrücklich schriftlich, dass der Lieferant dies tut, und Amazon behält sich das Recht vor, Form und Inhalt der Benachrichtigung zu überprüfen und zu genehmigen, bevor sie einer Partei gesandt wird. Der Lieferant arbeitet mit Amazon zusammen, um einen Plan zur Behebung aller bestätigten Sicherheitsvorfälle zu formulieren und auszuführen.

2.6.2 Soweit dies nach geltendem Recht zulässig ist, benachrichtigt der Lieferant Amazon rechtzeitig, wenn er eine Anfrage oder Anordnung einer Regierungsbehörde (wie z. B. Ladung, Gerichtsbeschluss oder Durchsuchungsbefehl) erhält, die Daten mit Amazon-Informationen anfordert, um es Amazon zu ermöglichen, eine Schutzanordnung oder eine andere angemessene Abhilfe zu beantragen.

2.7 Allgemeine Bestimmungen. Es liegt im alleinigen Ermessen von Amazon, alle im Rahmen dieser Sicherheitsrichtlinie geltenden Entscheidungen zu treffen. Eine Liste von Beispielen nach „einschließlich“ oder „z. B.“ ist illustrativ und nicht erschöpfend. Alle Verweise auf Standards für Sicherheitsanforderungen im Rahmen

dieser Sicherheitsrichtlinie beziehen sich auf die angegebenen Standards und ihre jeweiligen Nachfolgeversionen oder gleichwertige Versionen in der jeweils aktuellen Fassung, sofern Amazon nichts Anderweitiges angibt.