ANLAGE A
INFORMATIONSSICHERHEIT

1. **Geltungsbereich**

Diese Anlage A beschreibt die Anforderungen hinsichtlich der Informationssicherheit zwischen dem Kunden und Cisco sowie die technischen und organisatorischen Sicherheitsmaßnahmen, die Cisco implementiert hat, um die Personenbezogenen Daten zu schützen bevor mit einer Verarbeitung im Rahmen der Vereinbarung begonnen wird.

2. **Allgemeine Sicherheitsmaßnahmen**

Cisco hat angemessene technische und organisatorische Maßnahmen implementiert und wird diese aufrechterhalten, um die Personenbezogenen Daten vor unbeabsichtigtem Verlust oder Löschung, Zerstörung oder Abänderung, unbefugter Offenlegung oder Zugriff sowie widerrechtlicher Zerstörung zu schützen. Hiervon erfasst sind auch die in dieser Anlage A beschriebenen Richtlinien, Verfahren und internen Kontrollen für die Mitarbeiter von Cisco, die Ausrüstung und die Einrichtungen an den Standorten von Cisco, die jeweils bei der Umsetzung der Vereinbarung involviert sind.

3. **Allgemeine Compliance**

a. **Compliance.** Cisco muss Prozesse und Verfahren dokumentieren und implementieren, um Verstöße gegen rechtliche, gesetzliche, behördliche oder vertragliche Verpflichtungen im Zusammenhang mit der Informationssicherheit oder mit anderen Sicherheitsanforderungen zu vermeiden. Diese Prozesse müssen so konzipiert sein, dass sie angesichts des Risikos der Verarbeitung einen angemessenen Schutz Personenbezogener Daten bieten. Cisco muss die Informationssicherheit gemäß seinen eigenen Richtlinien und Verfahren implementieren und wahren, wobei die in diesem Anlage A genannten Anforderungen an die Informationssicherheit als Mindestmaß gelten.

b. **Schutz von Aufzeichnungen.** Cisco muss angemessene Maßnahmen implementieren, um die Aufzeichnungen in Übereinstimmung mit rechtlichen, behördlichen und vertraglichen Anforderungen vor Verlust, Zerstörung, Verfälschung, unbefugtem Zugriff und unbefugter Veröffentlichung zu schützen.

c. **Überprüfung der Informationssicherheit.** Das Management und die Implementierung der Informationssicherheit durch Cisco werden in geplanten Intervallen oder bei maßgeblichen Veränderungen durch geeignete interne oder externe Gutachter überprüft.

d. **Einhaltung von Sicherheitsrichtlinien und -standards.** Das Management von Cisco muss regelmäßig überprüfen, ob die Informationsverarbeitung und die Verfahren einschlägigen angemessenen Sicherheitsrichtlinien und -standards genügen.

e. **Überprüfung der technischen Compliance.** Cisco muss seine Informationssysteme regelmäßig auf Übereinstimmung mit den Richtlinien und Standards von Cisco in Bezug auf Informationssicherheit überprüfen.

f. **Informationsbezogenes Risikomanagement („IRM“).** Cisco muss einen angemessenen, im Einklang mit anwendbaren vertraglichen und rechtlichen Verpflichtungen stehenden Risikomanagementprozess in Bezug auf die Informationen implementieren und nutzen, um Risiken einzugrenzen, zu bewerten, auf sie zu reagieren und sie zu überwachen. Die Bewertung der Bedrohungen und Schwachstellen muss regelmäßig überprüft werden und dort, wo Schwachstellen entdeckt werden, müssen unverzüglich Gegenmaßnahmen ergriffen werden.

g. **Verarbeitung Besonderer Kategorien Personenbezogener Daten.** Sofern Cisco Besondere Kategorien Personenbezogener Daten verarbeitet und die in diesem Anlage A dargestellten Maßnahmen keinen hinreichenden Schutz bieten, kann der Kunde bei Cisco anfragen, dass Cisco zusätzliche Sicherheitsmaßnahmen implementiert.

Page Break

4. **Technische und organisatorische Sicherheitsmaßnahmen**

a. **Organisation der Informationssicherheit**

i. **Zuständigkeit für die Sicherheit.** Cisco muss mindestens einen Sicherheitsbeauftragten benennen, der für die Koordinierung und Überwachung der Sicherheitsanforderungen und -verfahren zuständig ist. Dieser Sicherheitsbeauftragte muss über die nötigen Kenntnisse, Erfahrungen und Befugnisse verfügen und die Verantwortung und Rechenschaftspflicht für die Informationssicherheit im Unternehmen zu übernehmen.

ii. **Rollen und Verantwortlichkeiten in Bezug auf die Sicherheit.** Cisco muss die Verantwortlichkeiten in Bezug auf die Informationssicherheit gemäß seinen eigenen genehmigten Informationssicherheitsrichtlinien definieren und zuweisen. Diese

Richtlinien müssen vollständig oder in Form von Zusammenfassungen veröffentlicht und den Mitarbeitern und relevanten externen Parteien, die zu ihrer Einhaltung verpflichtet sind, mitgeteilt werden.

iii. **Projektmanagement.** Cisco befasst sich mit der Informationssicherheit im Projektmanagement, um Informationssicherheitsrisiken zu identifizieren und angemessen anzugehen.

b. **Sicherheit im Personalwesen**

i. **Allgemein.** Cisco muss sicherstellen, dass Cisco Mitarbeiter zur Vertraulichkeit verpflichtet sind, sowie angemessene Schulungen über die relevanten Richtlinien und Verfahren in den Bereichen Datenschutz und Sicherheit anbieten. Darüber hinaus muss Cisco seine Mitarbeiter über mögliche Folgen von Verstößen gegen die Sicherheitsrichtlinien und -verfahren von Cisco in Kenntnis setzen. Zu diesen Folgen müssen Disziplinarmaßnahmen zählen, einschließlich der möglichen Kündigung festangestellter Mitarbeiter und einer Vertrags- oder Auftragsbeendigung für Vertreter und Zeitarbeitskräften.

ii. **Schulungen.** Cisco Mitarbeiter, die Zugriff auf Personenbezogene Daten haben, müssen jährlich in angemessenem Umfang hinsichtlich der bei der Erbringung der Services einzuhaltenden Datenschutz- und Sicherheitsverfahren geschult werden, damit sie in der Lage sind zu unterstützen, um unbefugte Nutzung oder unbeabsichtigte Offenlegung von Personenbezogenen Daten zu verhindern. Dies schließt Schulungen hinsichtlich des effektiven Umgangs mit Sicherheitsvorfällen ein. Die Schulungen müssen durchgeführt werden, bevor den Mitarbeitern von Cisco Zugriff auf die Personenbezogenen Daten gewährt wird bzw. bevor mit den Services begonnen wird. Die Schulungsinhalte sind regelmäßig durch Auffrischungskurse, E-Mails, Poster, schwarze Bretter und andere Schulungs- und Informationsmaterialien zu vertiefen.

iii. **Überprüfungen.** Cisco führt strafrechtliche und andere relevante Hintergrundüberprüfungen für sein Personal in Übereinstimmung mit den geltenden Gesetzen und den Richtlinien von Cisco durch.

c. **Zugriffskontrollen**

i. **Zugriff**

A. Beschränkte Nutzung. Cisco greift für keine anderen Zwecke auf die Computersysteme des Kunden zu als zur Erfüllung seiner Verpflichtungen aus der Vereinbarung und/ oder setzt Informationen zum Systemzugriff oder Anmeldeinformationen nicht ein, um sich unbefugt Zugriff auf Personenbezogene Daten oder auf die Computersysteme des Kunden zu verschaffen oder um den Umfang des befugten Zugriffs zu überschreiten.

B. Autorisierung. Cisco muss den Zugriff auf die Personenbezogenen Daten und Systeme des Kunden stets auf diejenigen Vertreter beschränken, die diesen Zugriff benötigen, um die Services und Produkte zu erbringen.

C. Aussetzung oder Entzug der Zugriffsrechte. Auf angemessene Anfrage des Kunden muss Cisco die Zugriffsberechtigungen seiner Mitarbeiter oder Vertreter zum Zugriff auf die Personenbezogenen Daten und Systeme ohne schuldhaftes Zögern unmittelbar aussetzen oder entziehen, wenn der begründete Verdacht besteht, dass die Cisco Mitarbeiter oder Vertreter gegen die Bestimmungen dieser Anlage A verstoßen haben. Außerdem muss Cisco allen Mitarbeitern und Vertretern die Zugriffsrechte entziehen, sobald das Beschäftigungsverhältnis oder die Beauftragung ausgesetzt oder beendet wird.

D. Klassifizierung von Informationen. Cisco muss Personenbezogene Daten klassifizieren, kategorisieren und/oder kennzeichnen, damit sie leichter zu erkennen sind und der Zugriff und die Nutzung angemessen beschränkt werden kann.

ii. **Zugriffsrichtlinie.** Cisco muss für jeden Benutzer angemessene Regeln, Berechtigungen und Beschränkungen für den Zugriff auf die Ressourcen festlegen. Cisco muss Aufzeichnungen über die Sicherheitsprivilegien von Mitarbeitern mit Zugriff auf Personenbezogene Daten, Netzwerke und Netzwerkservices führen. Cisco muss die Nutzung von Dienstprogrammen, die die System- und Anwendungskontrollen möglicherweise außer Kraft setzen können, beschränken und strikt kontrollieren.

iii. **Autorisierung des Zugriffs.**

A. Cisco muss Verfahren zum Erstellen und Löschen von Benutzerkonten, sowie entsprechende Genehmigungen zur Gewährung und Aufhebung von Zugriffsrechten auf die Systeme und Netzwerke des Kunden festlegen. Cisco muss ein unternehmensweites Zugriffskontrollsystem nutzen, bei dem die Manager ihre Mitarbeiter regelmäßig neu validieren müssen, wobei das Prinzip der „geringsten Rechte“ und des „Need-to-Know“ gilt und damit Benutzer nur den Zugriff erhalten, den sie für ihre Rolle im Unternehmen unbedingt benötigen.

B. Cisco muss Aufzeichnungen darüber führen und diese fortlaufend aktualisieren, welche Mitarbeiter zum Zugriff auf Systeme befugt sind, die Personenbezogene Daten enthalten. Außerdem sind die Zugriffsrechte der Benutzer regelmäßig zu überprüfen.

C. Bei Systemen, die Personenbezogene Daten verarbeiten, muss Cisco den Zugriff von Benutzern, deren Berichtsstruktur sich verändert, erneut validieren (oder falls angemessen deaktivieren). Authentifizierungsinformation, die während eines festzulegenden Zeitraums (maximal sechs (6) Monate) nicht genutzt wurden, sind zu deaktivieren.

D. Cisco muss Zugriffsbeschränkungen für den Quellcode von Programmen und zugehörige Ressourcen wie Softwareobjektcode, Designs, Spezifikationen, Verifizierungspläne und Validierungspläne einrichten, um die Implementierung nicht genehmigter Funktionen sowie unbeabsichtigte Änderungen zu verhindern. Netzwerkdesign. Bei Systemen zur Verarbeitung Personenbezogener Daten muss Cisco Kontrollen einrichten, die verhindern, dass sich Mitarbeiter Zugriffsrechte verschaffen, die über die ihnen zugewiesenen Zugriffrechte hinausgehen, und so unbefugt Zugriff auf Personenbezogene Daten erhalten.

iv. **Prinzip der geringsten Rechte.** Cisco muss den Zugriff auf Daten auf diejenigen Vertreter beschränken, die den tatsächlichen Bedarf haben, auf die Daten zuzugreifen, um die ihnen zugewiesenen Aufgaben zu erfüllen.

v. **Authentifizierung**

A. Cisco muss branchenübliche Verfahren einrichten, inklusive ISO/IEC 27002:2013 and NIST SP 800-63B (Digital Identity Guidelines) um Nutzer zu identifizieren und authentifizieren, die versuchen, sich Zugriff auf Informationssysteme zu verschaffen.

B. Bei kennwortbasierten Authentifizierungsmechanismen muss Cisco strikte Kontrollparameter für die Kennwörter vorschreiben (z. B. bezogen auf Länge, Komplexität der Zeichen und/oder Wiederverwendung), mit mindestens 8 Zeichen und folgende vier Kategorien enthaltend:
Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen.

C. Cisco muss sicherstellen, dass deaktivierte oder abgelaufene Kennungen und Anmeldeinformationen nicht an andere Personen vergeben werden.

D. Cisco muss auf wiederholt fehlgeschlagene Zugriffsversuche auf das Informationssystem überwachen.

E. Cisco muss branchenübliche Verfahren zum Deaktivieren von manipulierten oder unbeabsichtigt offengelegten Anmeldeinformationen nutzen.

F. Cisco muss branchenübliche Verfahren zum Schutz von Anmeldeinformationen verwenden, einschließlich solcher, die auf die Aufrechterhaltung der Vertraulichkeit und Integrität der Anmeldeinformationen, beim Zuweisen und Verteilen, sowie bei der Speicherung, ausgelegt sind (z. B. dürfen Anmeldeinformationen nicht in Klartext gespeichert oder weitergegeben werden). Diese Verfahren sind so zu gestalten, dass sie für sichere, vertrauliche Anmeldeinformationen sorgen.

G. Cisco muss eine Multi-Faktor-Authentifizierungslösung implementieren, um das Personal zu authentifizieren, das auf seine Informationssysteme zugreift.

d. **Physische Sicherheit und Sicherheit in der Umgebung**

i. **Physischer Zugang zu Einrichtungen**

A. Cisco muss den Zugang zu Einrichtungen, in denen sich Systeme zur Verarbeitung Personenbezogener Daten befinden, auf die befugten Personen beschränken.

B. Zum Schutz von Bereichen, in denen sich sensible oder kritische Informationen sowie Einrichtungen zur Verarbeitung befinden, sind Sicherheitszonen zu definieren und einzuhalten.

C. Einrichtungen müssen durchgehend (24 Stunden am Tag, 7 Tage pro Woche) überwacht werden, und der Zugang zu ihnen ist zu kontrollieren. Die Zugangskontrolle muss per Schlüsselkarte erfolgen und/oder anhand angemessener Anmeldeverfahren für Einrichtungen mit Systemen zur Verarbeitung Personenbezogener Daten. Cisco muss seine Mitarbeiter registrieren und zum Tragen geeigneter Firmenausweise verpflichten.

ii. **Physischer Zugang zur Ausrüstung.** Die Ausrüstung von Cisco, die zur Verarbeitung oder Speicherung Personenbezogener Daten verwendet wird, muss mit **branchenüblichen Prozessen zum Beschränken des Zugangs auf befugte Personen ausgestattet sein.**

iii. **Schutz vor Unterbrechungen.** Cisco muss angemessene Maßnahmen zum Schutz vor Datenverlusten durch Stromausfälle oder Störungen treffen.

iv. **Aufgeräumter Arbeitsplatz (Clean Desk). Cisco muss über Richtlinien für einen aufgeräumten Arbeitsplatz bzw. Bildschirm verfügen, um die unbeabsichtigte Offenlegung Personenbezogener Daten zu verhindern.**

e. **Betriebssicherheit**

i. **Betriebsrichtlinie.** Cisco muss seine Sicherheitsmaßnahmen und die relevanten Verfahren und Verantwortlichkeiten seiner Mitarbeiter mit Zugriff auf die Personenbezogenen Daten sowie die entsprechenden Systeme und Netzwerke schriftlich in erläuternden Richtlinien festhalten. Die Richtlinien und Anforderungen sind von Cisco an alle in die Verarbeitung Personenbezogener Daten involvierten Personen zu kommunizieren. Cisco muss eine geeignete Managementstruktur und Kontrolle implementieren, um die Einhaltung dieser Richtlinien und zwingend geltender Gesetze zum Schutz und zur Verarbeitung Personenbezogener Daten zu gewährleisten.

ii. **Sicherheits- und Verarbeitungskontrollen.**

A. Bereiche. Cisco muss Standards und Verfahren zur Konfiguration, zum Betrieb und zur Verwaltung von Systemen, Netzwerken und Leistungen, auf bzw. mit denen Personenbezogene Daten gespeichert oder verarbeitet werden, pflegen, dokumentieren und implementieren.

B. Standards und Verfahren. Diese Standards und Verfahren müssen Folgendes abdecken: Sicherheitskontrollen, Ermittlung und Patching von Sicherheitsschwachstellen, Prozess und Verfahren zur Änderungskontrolle sowie Verhinderung, Erkennung, Behebung und Management von Vorfällen.

iii. **Protokollierung und Überwachung.** Cisco muss Administrator- und Betreiberaktivitäten sowie Datenwiederherstellungsereignisse im Zusammenhang mit Personenbezogenen Daten protokollieren.

f. **Kommunikationssicherheit und Datenübermittlung**

i. **Netzwerke.** Cisco muss seine Netzwerke für den Zugriff und die Verarbeitung Personenbezogener Daten mindestens mit folgenden Kontrollen absichern:

A. Der Netzwerkdatenverkehr muss Firewalls durchlaufen, die durchgehend überwacht werden. Cisco muss Intrusion-Erkennung-Systeme und/oder Intrusion-Prevention-Systeme implementieren.

B. Auf den Routern müssen Anti-Spoofing-Filter aktiviert werden.

C. Die Kennwörter zur Netzwerk-, Anwendungs- und Serverauthentifizierung müssen gleiche

D. Industriestandardpraktiken, die für die Authentifizierung von Benutzern verwendet werden, wie in Abschnitt 4.34.3.f oben beschrieben (Authentifizierung). Passwörter auf Systemebene (privilegierte Administratorkonten oder Benutzerkonten mit privilegiertem Administratorzugriff) müssen mindestens alle 90 Tage geändert werden.

E. Die Benutzer müssen verpflichtet werden, ihre anfänglichen Kennwörter bei der ersten Anmeldung zu ändern. Cisco muss mit einer Richtlinie die Weitergabe von Benutzer-IDs, Kennwörtern oder anderen Anmeldeinformationen verbieten.

F. Die Außenstellen (perimeter) der Netzwerke von Cisco müssen mit Firewalls geschützt werden.

ii. **Virtual Private Networks ("VPN").** Wenn zur Verarbeitung Personenbezogener Daten Remote-Verbindungen zum Netzwerk des Kunden oder zum Netzwerk von Cisco erforderlich sind, gilt Folgendes:

A. Die Verbindungen müssen mit branchenüblicher Kryptografie verschlüsselt werden.
B. Verbindungen dürfen nur über VPN-Server hergestellt werden.
C. Der Einsatz von Multi-Faktor-Authentifizierung ist erforderlich.

iii. **Datenübermittlung.** Cisco muss über formelle Datenübermittlungsrichtlinien zum Schutz der Übertragung von Informationen über Kommunikationsvorrichtungen aller Art verfügen, die den Anforderungen dieser Anlage A genügen. Diese Richtlinien sollen die übertragenen Informationen vor dem unbefugten Abfangen, Kopieren, Modifizieren, Manipulieren, Routen und Zerstören schützen.

g. **Beschaffung, Entwicklung und Wartung von Systemen**

i. **Sicherheitsanforderungen.** Cisco muss Sicherheitsanforderungen für den Erwerb, die Nutzung und die Entwicklung von Informationssystemen festlegen. Dies gilt u. a. für über öffentliche Netzwerke bereitgestellte Anwendungsservices.

ii. **Entwicklungsanforderungen.** Cisco muss über Richtlinien für sichere Entwicklung, Systemtechnik und Support verfügen. Im Rahmen der Prozesse für Akzeptanztests muss Cisco auch angemessene Tests der Systemsicherheit durchführen. Bei einer Auslagerung der Systementwicklung muss Cisco sämtliche Aktivitäten beaufsichtigen und überwachen.

h. **Penetrationstests, Überprüfungen auf Schwachstellen, Audit-Berichte**

i. **Tests.** Cisco muss regelmäßig Schwachstellen-Scans und Penetrationstests für sein Internetperimeternetzwerk durchführen. Diese Scans und Tests werden von hochqualifizierten Fachleuten durchgeführt, darunter auch das Compliance-Team von Cisco. Dabei werden branchenübliche Tools und Methoden verwendet.

ii. **Audits und Zertifizierungen.** Cisco kooperiert bei berechtigten Anfragen des Kunden nach Audits zur Überprüfung der Einhaltung von Datenschutzgesetzen (vorbehaltlich gegenseitiger Vereinbarung über Zeitpunkt, Dauer, Ort, Umfang und Art der Audits, es sei denn, ein unangekündigtes Audit ist notwendig) und kommt angemessenen Anfragen nach Testberichten und Zertifizierungen nach. Cisco stellt dem Kunden auf schriftliche Anfrage und unverzüglich Kopien von Auditberichten oder Drittzertifizierungen zur Verfügung, die es verwaltet (z.B. SSAE 16 – SOC1-, SOC2-, SOC3- Bescheinigungen oder ISO 27001:2013-Zertifizierungen (oder deren Äquivalente bzw. Nachfolgestandards)), die für den Service oder das Produkt des Kunden relevant sind, sofern Cisco solche Zertifizierungen im normalen Geschäftsverlauf beibehält. Der Kunde behandelt den Inhalt der Testberichte und Auditreports vertraulich, sofern zwischen den Parteien nicht etwas anderes vereinbart wird.

iii. **Abhilfemaßnahme.** Wenn bei einem Penetrationstest oder einem Schwachstellenscan gemäß Abschnitt 4 (h) (i) Mängel, Schwachstellen oder Bereiche der Nichteinhaltung festgestellt werden, muss Cisco nach vernünftigem Ermessen unverzüglich die erforderlichen Maßnahmen ergreifen, um die wesentlichen Mängel, Schwachstellen und Bereiche der Nichteinhaltung, zu beheben, sobald dies unter Berücksichtigung der Priorisierung durch Cisco aufgrund ihrer Kritikalität (z. B. Art, Schweregrad, Wahrscheinlichkeit) praktikabel ist.

iv. **Status der Abhilfemaßnahmen.** Nach Aufforderung durch den Kunden muss Cisco den Kunden über den Status der erforderlichen Abhilfemaßnahmen auf dem Laufenden halten. Hierbei ist auch der geschätzte Zeitplan bis zum Abschluss der Maßnahmen zu nennen.

i. **Einsatz von Vertretern**

i. **Richtlinien.** Cisco muss über Informationssicherheitsrichtlinien oder -verfahren verfügen, die beim Einsatz von Vertretern den Anforderungen dieser Anlage A entsprechen.

ii. **Überwachung.** Cisco muss die Servicebereitstellung durch Auftragnehmer überwachen und die Sicherheitspraktiken seiner Auftragnehmer in Bezug auf die in den Vereinbarungen von Cisco mit diesen Auftragnehmern festgelegten Sicherheitsanforderungen überprüfen.

j. **Vorgehen bei der Verletzung des Schutzes Personenbezogener Daten und Verbesserungsmaßnahmen**

i. **Verantwortlichkeiten und Verfahren.** Cisco muss Verfahren etablieren, die eine schnelle, effektive und geregelte Reaktion bei Verletzungen des Schutzes Personenbezogener Daten gewährleisten.

ii. **Meldung von Verletzungen des Schutzes Personenbezogener Daten.** Cisco

muss Verfahren implementieren, damit Verletzungen des Schutzes Personenbezogener Daten so schnell wie vernünftigerweise möglich gemeldet werden. Allen Mitarbeitern und Vertretern soll ihre Verantwortung bewusst gemacht werden, Verletzungen des Schutzes Personenbezogener Daten so schnell wie vernünftigerweise möglich zu melden.

iii. **Meldungen über Schwachstellen der Informationssicherheit.** Cisco, seine Mitarbeiter und seine Vertreter müssen alle in Systemen oder Services beobachteten oder vermuteten Schwachstellen der Informationssicherheit dokumentieren und melden.

iv. **Bewertung undEinordnung von Schwachstellen der Informationssicherheit.** Cisco muss über eine Skala zur Klassifizierung von Vorfällen verfügen, aus der sich ablesen lässt, ob ein Sicherheitsvorfall als Verletzung des Schutzes Personenbezogener Daten einzuordnen ist. Die Klassifizierungsskala richtet sich nach dem Umfang und den Auswirkungen einer Schwachstelle.

v. **Erfassung und Umgang mit Verletzungen des Schutzes Personenbezogener Daten.** Cisco muss Aufzeichnungen über Verletzungen des Schutzes Personenbezogener Daten unterhalten, die eine Beschreibung des Vorfalls, der Auswirkungen, den Namen desjenigen der den Vorfall meldet sowie desjenigen der diese Meldung, des Verfahrens zur Reaktion auf den Vorfall und die Maßnahmen zum Verhindern künftiger Sicherheitsvorfälle.

k. **Aspekte der Informationssicherheit bei der Aufrechterhaltung des ungestörten Betriebsablaufs (Business Continuity Management)**

i. **Planung.** Cisco muss über Notfallpläne für die Einrichtungen verfügen, in denen sich seine Informationssysteme befinden, die Personenbezogene Daten verarbeiten. Cisco muss die festgelegten und implementierten Kontrollen zur Kontinuität der Informationssicherheit regelmäßig verifizieren.

ii. **Datenwiederherstellung.** Cisco muss redundante Speicherverfahren und Methoden entwickeln, um Personenbezogene Daten in einer Weise wiederherstellen zu können, damit sie dem Zustand entsprechen, wie er auf der letzten aufgezeichneten, vom Kunden bereitgestellten Sicherung gefunden wurde, oder in einer Weise, die ausreicht, um den Service wieder aufzunehmen.