CISCO MASTER DATA PROTECTION AGREEMENT/ VEREINBARUNG ÜBER DIE AUFTRAGSDATENVERARBEITUNG

Dieses Cisco Master Data Protection Agreement/ Vereinbarung über die Auftragsdatenverarbeitung, nachfolgend „**ADV**") wird geschlossen zwischen Freie Universität Berlin, Kaiserswerther Str. 16/18, 14195 Berlin, Deutschland ("**Kunde**") im eigenen Namen und soweit unter den Datenschutzgesetzen (gemäß der untenstehenden Definition) erforderlich, im Namen seiner Verbundenen Unternehmen (im Sinne der nachfolgend definierten Vereinbarung) und der Cisco International Limited, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex TW14 8HA, United Kingdom ("**Cisco**") und seinen Verbundenen Unternehmen (einzeln jeweils als „**Partei**" und gemeinsam als die „**Parteien**" bezeichnet).

Die ADV tritt ab dem Datum der letzten Unterschrift in Kraft („**Datum des Inkrafttretens**"), gehört zu der nachfolgend definierten Vereinbarung und findet insoweit Anwendung, als Cisco Personenbezogene Daten als Auftragsverarbeiter des Kunden bei der Bereitstellung von Produkten und / oder Services (gemäß der untenstehenden Definition) im Hinblick auf die Vereinbarung verarbeitet.

Sofern in dieser ADV nicht anderweitig geregelt, bleiben die Bestimmungen der Vereinbarung durch diese ADV unberührt. Alle in dieser ADV nicht definierten Begriffe in Großschreibung haben die in der Vereinbarung festgelegte Bedeutung. Alle zuvor von Cisco und dem Kunden getroffenen Regelungen oder Vereinbarungen im Hinblick auf den Schutz und die Sicherheit Personenbezogener Daten werden durch den Abschluss dieser ADV ersetzt. Im Falle eines Widerspruchs zwischen dieser ADV und der Vereinbarung haben die Regelungen dieser ADV Vorrang.

1) DEFINITIONEN

a. „**APEC**" bezeichnet die Asiatisch-Pazifische Wirtschaftsgemeinschaft (Asian-Pacific Economic Cooperation), ein regionales Wirtschaftsforum, das 1989 gegründet wurde, um die wachsende gegenseitige Abhängigkeit des asiatisch-pazifischen Raums zu nutzen. Weitere Informationen finden Sie unter www.apec.org.

b. „**APEC Mitglieder**" bezeichnet die 21 Mitglieder der APEC: Australien, Brunei Darussalam, Kanada, Chile, China, Hongkong-China, Indonesien, Japan, Republik Korea, Malaysia, Mexiko, Neuseeland, Papua-Neuguinea, Peru, Philippinen, Russland, Singapur, Chinesisch-Taipeh, Thailand, USA und Vietnam.

c. „**Aufsichtsbehörde**" bezeichnet eine von einem Mitgliedstaat eingerichtete unabhängige staatliche Stelle gemäß DSGVO.

d. "**Auftragsverarbeiter**" bezeichnet eine juristische Person, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

e. „**Besondere Kategorien Personenbezogener Daten**" sind Daten, die die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Mitgliedschaft in einer Gewerkschaft sowie die Verarbeitung genetischer und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person offenlegen, sowie Gesundheitsdaten, Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person, bestimmte Finanzinformationen, wenn sie durch anwendbares zwingendes Recht als solche gekennzeichnet sind, genaue zeitliche Geolokalisierung und Daten im Zusammenhang mit Straftaten oder strafrechtlichen Verurteilungen.

f. "**Betroffene Person**" bezeichnet die Person, auf die sich die Personenbezogenen Daten beziehen.

g. "**Datenschutzgesetze**" bezeichnen alle zwingend auf die Verarbeitung Personenbezogener Daten anwendbaren Gesetze, einschließlich des Rechts der Europäischen Union und der Mitgliedstaaten der Europäischen Union.

h. "**DSGVO**" bezeichnet die Verordnung 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung).

i. „**EWR**" oder „**Europäischer Wirtschaftsraum**" bezeichnet die Länder, die Mitglied der Europäischen Freihandelsassoziation (EFTA = European Free Trade Association) sind, sowie die Länder, die zum gegebenen Zeitpunkt Mitglied der Europäischen Union sind (d. h. ihr beigetreten sind).

j. „**Genehmigte Gerichtsbarkeit**" bezeichnet einen Mitgliedstaat des EWR oder eine andere Gerichtsbarkeit, die von der Europäischen Kommission als angemessener Rechtsschutz für Daten anerkannt wurde. Eine Übersicht findet sich hier:https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

k. "**Personenbezogene Daten**" bezeichnet alle Informationen, über oder in Bezug auf eine identifizierte oder identifizierbare natürliche Person. Dies beinhaltet alle Informationen, die mit einer natürlichen Person verknüpft oder zu ihrer direkten oder indirekten Identifizierung verwendet werden können.

l. „**Privacy Data Sheet(s)**" bezeichnet das einschlägige Dokument im Cisco's Trust Portal, welches die Verarbeitung in Bezug auf den oder die jeweiligen Service(s) beschreibt.

m. "**Produkt**" bezeichnet die von Cisco oder seinen Verbundenen Unternehmen gekennzeichnete Hardware und / oder Software, die vom Kunden im Rahmen der Vereinbarung erworben wurde.

n. "**Service**" bezeichnet eine von Cisco oder seinen Verbundenen Unternehmen gekennzeichnete Dienstleistung, die von Kunden im Rahmen der Vereinbarung erworben wurde.

o. „**Standardvertragsklauseln**" bezeichnet die in Anlage C zu dieser ADV enthaltene Vereinbarung, die von der Europäischen Kommission für den Transfer Personenbezogener Daten an in Drittländern ansässige Auftragsverarbeiter genehmigt wurde, die kein angemessenes Datenschutzniveau bieten.

p. "**Verantwortlicher**" bezeichnet eine juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Personenbezogenen Daten entscheidet.

q. „**Verarbeiten**" bezeichnet alle Vorgänge oder Vorgangsreihen, die auf Personenbezogene Daten angewendet werden, mit oder ohne Hilfe automatisierter Verfahren, wie das Erheben, das Erfassen, die Sicherung, die Organisation, die Speicherung, die Anpassung oder Änderung, den Zugriff, den Abruf, die Auswertung, die Nutzung, die Offenlegung durch Übertragung, die Weitergabe oder sonstige Arten der Verfügbarmachung, den Abgleich oder die Kombination, die Sperrung, die Löschung oder die Zerstörung. Der Begriff der „**Verarbeitung**" ist jeweils gleichermaßen in diesem Sinne zu verstehen.

r. „**Verbundene Unternehmen**" bezeichnet jedes Unternehmen, das direkt oder indirekt von der betreffenden Partei kontrolliert wird oder unter gemeinsamer Kontrolle mit der betreffenden Partei steht, wobei „Kontrolle" bedeutet: (a) dass die betreffende Partei mehr als 50% des Unternehmens besitzt; oder (b) in der Lage ist, die Angelegenheiten der betreffenden Partei durch rechtmäßige Mittel (z. B. einen Vertrag, der die Kontrolle ermöglicht) zu lenken. Zu diesen Verbundenen Unternehmen gehören Cisco Systems, Inc., Cisco Commerce India Private Limited, Cisco Systems G.K., Cisco Systems Australia PTY Limited, Cisco Systems Canada Co., Cisco International Limited, Cisco Systems (Italien) S.R.L. und Cisco Systems International BV. Sofern von den Parteien nicht ausdrücklich anders vereinbart, stellen Meraki LLC, AppDynamics LLC und ThousandEyes, Inc. sowie juristische Personen, die durch eine Akquisition oder Fusion Teil der Cisco-Unternehmensgruppe geworden sind, keine Verbundenen Unternehmen unter dieser ADV dar.

s. „**Vereinbarung**" bezeichnet die schriftliche oder elektronische Vereinbarung zwischen dem Kunden und Cisco oder dem betreffenden Verbundenen Unternehmen von Cisco für die Bereitstellung der Services und / oder Produkte für den Kunden.

t. „**Verletzung des Schutzes Personenbezogener Daten**" bezeichnet eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang zu Personenbezogenen Daten führt.

u. „**Vertreter**" bezeichnet die Führungskräfte, Direktoren, Mitarbeiter, Vertreter, Auftragnehmer, Zeitarbeitskräfte, Subunternehmer und Berater der jeweiligen Partei sowie ihrer Verbundenen Unternehmen.

v. „**Unterauftragsverarbeiter**" bezeichnet einen anderen Auftragsverarbeiter, der von Cisco oder seinen Verbundenen Unternehmen in die Verarbeitung der Personenbezogenen Daten des Kunden eingesetzt wird.

2) BESCHREIBUNG DER VERARBEITUNG

Cisco verarbeitet Personenbezogene Daten wie in Anlage B dieser ADV beschrieben (Zweck, Umfang, Kategorien der Personenbezogenen Daten und Betroffene Personen).

3) VERPFLICHTUNGEN DER PARTEIEN

a. Die Parteien vereinbaren, dass in Bezug auf die Personenbezogenen Daten der Kunde der Verantwortliche und Cisco der Auftragsverarbeiter ist.

b. Der Kunde muss:

i. bei der Nutzung der Produkte und / oder Services die geltenden Datenschutzgesetze einhalten;

ii. sicherstellen, dass alle Weisungen, die Cisco vom Kunden in Bezug auf die Verarbeitung von Personenbezogene Daten erhält, nicht gegen die Datenschutzgesetze verstoßen;

iii. sicherstellen, dass alle an Cisco übermittelten Personenbezogenen Daten gemäß den Datenschutzgesetzen erhoben wurden und dass der Kunde über alle erforderlichen Berechtigungen und / oder Einwilligungen verfügt, um Cisco diese Personenbezogenen Daten zur Verfügung zu stellen; und

iv. der Umfang der Personenbezogenen Daten, die er Cisco übermittelt oder zugänglich macht, auf das Minimum beschränken, das für die Zurverfügungstellung der Produkte und/oder der Services erforderlich ist.

c. Cisco muss:

i. die Personenbezogenen Daten gemäß den dokumentierten Weisungen des Kunden, den Standardvertragsklauseln und dieser ADV verarbeiten, jedoch nur in dem Umfang, in dem die Weisungen im Einklang mit den Datenschutzgesetzen stehen. Cisco wird den Kunden umgehend benachrichtigen, wenn Cisco der Ansicht ist, dass die Weisungen des Kunden nicht mit den Datenschutzgesetzen im Einklang stehen;

ii. soweit eine Verarbeitung Personenbezogener Daten aufgrund von Datenschutzgesetzen, Gerichtsbeschlüssen, Anordnungen oder anderen rechtlichen oder gerichtlichen Verfahren erforderlich ist, die nicht im Einklang mit den Weisungen den Kunde stehen, den Kunden über das entsprechende Erfordernis benachrichtigen, es sei denn, das anwendbare zwingende Recht verbietet eine solche Benachrichtigung aus wichtigen Gründen des öffentlichen Interesses;

iii. sicherstellen, dass seine berechtigten Vertreter, die ggf. Personenbezogene Daten verarbeiten, schriftliche vertragliche Verpflichtungen mit Cisco eingegangen sind, um die Personenbezogenen Daten geheim zu halten;

iv. einen Datenschutzbeauftragten benennen. Cisco wird die Kontaktdaten des Datenschutzbeauftragten auf Verlangen herausgeben;

v. den Kunden im Bedarfsfall bei der Beantwortung von Anfragen von Aufsichtsbehörden, Betroffenen Personen, Kunden oder anderen Personen unterstützen, um Informationen bereitzustellen, die sich auf die Verarbeitung Personenbezogener Daten durch Cisco beziehen;

vi. Personenbezogene Daten in seinen Systemen oder Einrichtungen nur in dem Umfang verarbeiten, wie dies zur Erfüllung der Verpflichtungen aus der Vereinbarung erforderlich ist;

vii. sofern anwendbar, als Unterauftragsverarbeiter für die Personenbezogenen Daten agieren;

viii. Aufzeichnungen über die Verarbeitung aller Personenbezogenen Daten des Kunden bereithalten, die Cisco im Rahmen der Vereinbarung erhalten hat;

ix. es unterlassen, Personenbezogene Daten zu vermieten, zu verkaufen, zu verbreiten oder anderweitig darüber zu verfügen, außer es wurde eine gesonderte schriftliche, von beiden Parteien unterzeichnete Vereinbarung hierüber getroffen;

x. den Kunden nach Aufforderung im Rahmen seiner Befähigungen im Hinblick auf die Erfüllung aller anwendbaren Anmelde-, Genehmigungs- oder ähnlichen Anforderungen der Datenschutzgesetze unterstützen;

xi. unter Berücksichtigung der Art der Verarbeitung und der Informationen, die Cisco zur Verfügung stehen, Informationen und Unterstützung bereitstellen, die der Kunde benötigt, um die Datenschutzgesetze in Bezug auf Folgendes einzuhalten:

A. Sicherheit der Verarbeitung;

B. Datenschutz-Folgeabschätzung (gemäß der Definition der DSGVO);

C. vorherige Konsultation einer Aufsichtsbehörde in Bezug auf die Verarbeitung mit einem hohen Risiko; und

D. Benachrichtigungen der zuständigen Aufsichtsbehörde und / oder Mitteilungen an Betroffene Personen durch den Kunden als Reaktion auf eine Verletzung des Schutzes Personenbezogener Daten;

xii. bei Beendigung der ADV, gleich aus welchem Grund, und nach Ende der Bereitstellung des Service – die Verarbeitung einstellen und alle vom Kunden erhaltenen Personenbezogenen Daten löschen, oder nach schriftlicher Aufforderungen des Kunden unverzüglich sämtliche Personenbezogenen Daten, die sich im Besitz oder unter der Kontrolle von Cisco befinden, zurückgeben und alle bestehenden Kopien sicher löschen, es sei denn, eine fortgesetzte Speicherung oder Verarbeitung stehen im Einklang mit den Datenschutzgesetzen. Auf Anforderung des Kunden muss Cisco die Einhaltung der Regelungen dieser Ziffer 2 (c) (xii) bestätigen.

4) ÜBERMITTLUNG PERSONENBEZOGENER DATEN

a. Übermittlung Personenbezogener Daten aus dem EWR oder der Schweiz oder dem Vereinigten Königreich in Drittländer. Wenn Cisco Personenbezogene Daten des Kunden aus dem EWR, der Schweiz oder dem Vereinigten Königreich in einem Land verarbeitet, das keine Genehmigte Gerichtsbarkeit darstellt, führt Cisco diese Verarbeitung gemäß den Standardvertragsklauseln und gemäß den Artikeln 44 ff. DSGVO durch.

b. Übermittlung Personenbezogener Daten aus anderen Regionen als dem EWR oder der Schweiz oder dem Vereinigten Königreich. Auch aus anderen Regionen als dem EWR, der Schweiz oder dem Vereinigte Königreich darf Cisco keine Personenbezogenen Daten aus einer Region heraus übermitteln, in der die Personenbezogenen Daten erhoben wurden, soweit dies nicht nach den Datenschutzgesetzen zulässig ist.

Wenn Cisco im Namen des Kunden Personenbezogene Daten aus einem Mitgliedsland der APEC verarbeitet, muss Cisco dabei die Anforderungen des APEC Cross Border Privacy Rules-Systems („**CBPR**", siehe www.cbprs.org) erfüllen, sofern diese auf die Verarbeitung der jeweiligen Personenbezogenen Daten anwendbar sind. Wenn Cisco das von den CBPR verlangte Maß an Sicherheit nicht sicherstellen kann, muss Cisco den Kunden sofort benachrichtigen und die Verarbeitung einstellen. In einem solchen Fall kann der Kunde die der Verarbeitung zugrundeliegende Vereinbarung durch schriftliche Mitteilung innerhalb von dreißig (30) Tagen beenden.

5) UNTERAUFTRAGSVERARBEITUNG

a. Der Kunde erteilt Cisco eine allgemeine Genehmigung zur Nutzung von Unterauftragnehmern und stimmt der Nutzung der in Anhang 1 zu Anlage B aufgeführten Unterauftragnehmer zu.

b. Cisco darf seine Verpflichtungen aus dieser ADV weder ganz noch teilweise an neue Unterauftragsverarbeiter vergeben, ohne dies dem Kunden vorher mitzuteilen (z. B. per E-Mail oder In-Application-Messaging). Wenn der Kunde dem vorgeschlagenen Unterauftrag aus wichtigen Gründen des Schutzes der Personenbezogenen Daten nicht zustimmt und die Parteien die Meinungsverschiedenheit nicht auflösen können, kann der Kunde den betreffenden Teil der Vereinbarung, der sich auf die Produkte und/oder Services bezieht, die Cisco ohne die Verwendung des Unterauftragverarbeiters nicht bereitstellen kann, mit einer Frist von dreißig (30) Tagen schriftlich kündigen.

c. Wenn Cisco einen Unterauftragsverarbeiter ernennt, schließt Cisco eine schriftliche Vereinbarung mit diesem Unterauftragsverarbeiter ab, deren Bedingungen dem Schutzniveau dieser ADV entsprechen.

d. Cisco ist für das Handeln und / oder Unterlassen von Unterauftragsverarbeitern in demselben Maße haftbar, wie für eigene Handlungen und / oder Unterlassungen unter dieser ADV.

e. Für die Zwecke der Klausel 11 der Standardvertragsklauseln erteilt der Kunde Cisco eine allgemeine Zustimmung zur Beauftragung von Unterauftragsverarbeitern. Diese Zustimmung steht unter der Bedingung, dass Cisco die Regelung dieser Ziffer 5 einhält.

6) RECHTE DER BETROFFENEN PERSONEN

Cisco muss den Kunden im gesetzlich zulässigen Umfang unverzüglich benachrichtigen, wenn eine Betroffene Person den Zugriff, die Korrektur, die Übertragung oder Löschung ihre(r) Personenbezogenen Daten beantragt. Sofern in den Datenschutzgesetzen nicht zwingend vorgegeben, darf Cisco nicht ohne vorherige schriftliche Zustimmung des Kunden auf Anfragen von Betroffenen Personen antworten, außer um zu bestätigen, dass sich die Anfrage auf den Kunden bezieht. Darüber hinaus wird Cisco alle Informationen bereitstellen, Kooperation anbieten und Maßnahmen ergreifen, die der Kunde in Bezug auf die Anfrage einer Betroffenen Person anfordert.

7) SICHERHEIT DER DATENVERARBEITUNG

Cisco muss geeignete technische und organisatorische Maßnahmen zum Schutz der Personenbezogenen Daten gemäß Art.32 DSGVO und mindestens die Maßnahmen in Anlage A implementieren und aufrechterhalten. Cisco überwacht regelmäßig die Einhaltung dieser technisch organisatorischen Maßnahmen.

8) AUDIT

a. Cisco stellt dem Kunden diejenigen Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Verpflichtungen dieser ADV und der Datenschutzgesetze durch Cisco nachzuweisen (zusätzlich zu den Informationen, die auf dem Cisco Trust Portal und in den Data Privacy Sheets enthalten sind). Cisco gestattet und unterstütz ein Audit nach Maßgabe von Anlage A, Ziffer 4 (h) (ii) dieser ADV.

b. Der Kunde erkennt an und stimmt zu, dass jede Ausübung seiner Auditrechte gemäß Ziffer 5 (f) der Standardvertragsklauseln nach Maßgabe dieser ADV durchgeführt wird.

9) BENACHRICHTIGUNG UND KOMMUNIKATION

a. **Benachrichtigung**. Cisco benachrichtigt den Kunden unverzüglich unter zedat@fu-berlin.de, spätestens jedoch innerhalb von 48 Stunden nach Bestätigung einer Verletzung des Schutzes Personenbezogener Daten des Kunden. Cisco stellt zeitnah alle Informationen und zur Verfügung erbringt alle Mitwirkungshandlungen, die der Kunde im Einzelfall benötigt, damit der Kunde seine Verpflichtungen zur Meldung einer Verletzung des Schutzes Personenbezogener Daten gemäß den Datenschutzgesetzen (und innerhalb der geforderten Fristen) erfüllen kann. Cisco wird ferner diejenigen Maßnahmen ergreifen, die Cisco für erforderlich hält, um die Auswirkungen der Verletzung des Schutzes Personenbezogener Daten zu beheben oder zu abzumildern, und den Kunden im Zusammenhang mit der Verletzung des Schutzes Personenbezogener Daten auf dem Laufenden halten.

b. **Kommunikation über die Informationssicherheit.** Sofern nicht aufgrund zwingend geltender Gesetze erforderlich, wird Cisco ohne die vorherige schriftliche Zustimmung des Kunden keine Dritten über die Verletzung des Schutzes Personenbezogener Daten informieren, durch die auf den Kunden verwiesen oder durch die der Kunde identifiziert wird. Cisco kooperiert mit dem Kunden und den Strafverfolgungsbehörden in Bezug auf die Verletzungen des Schutzes Personenbezogener Daten. Cisco bewahrt für einen angemessenen Zeitraum alle Informationen und Daten auf, die sich im Besitz oder unter oder Kontrolle von Cisco, und im direkten Zusammenhang mit einer Verletzung des Schutzes Personenbezogener Daten stehen. Wenn die Offenlegung der Verletzung des Schutzes Personenbezogener Daten zwingend gesetzlich vorgeschrieben ist, wird Cisco im Hinblick auf die zeitliche Planung, Inhalte und Empfänger der Offenlegung mit dem Kunden zusammenarbeiten.

c. **Pflichten nach der Verletzungen des Schutzes Personenbezogener Daten.** Nach einem Vorfall wird Cisco mit dem Kunden bei der Aufklärung, bei Abhilfemaßnahmen und der Kommunikation im vernünftigen Umfang zusammenarbeiten.

d. Änderungen bei der Verarbeitung Personenbezogener Daten des Kunden gemäß dieser ADV werden dem Kunden durch Cisco schriftlich (per Brief) oder in elektronischer Form (per E-Mail oder In-Application Messaging) mitgeteilt. Über unwesentliche Anpassungen des Service oder Produkts, z.B. Updates, Upgrades und Features wird der Kunden über die Privacy Data Sheet(s) oder über In-Application-Messaging informiert.

10) BESCHWERDEN ODER BENACHRICHTIGUNGEN IN BEZUG AUF PERSONENBEZOGENE DATEN

Wenn Cisco eine offizielle Beschwerde, Benachrichtigung oder Mitteilung erhält, die sich auf die Verarbeitung von Personenbezogener Daten durch Cisco oder auf die Einhaltung der Datenschutzgesetze durch eine Partei im Zusammenhang mit den Personenbezogenen Daten bezieht, wird Cisco den Kunden, soweit gesetzlich zulässig, unverzüglich benachrichtigen und dem Kunden seine Kooperation und Unterstützung in Bezug auf die betreffenden Beschwerden, Benachrichtigungen oder Mitteilungen anbieten.

11) HAFTUNG

a. Nichts in dieser ADV beschränkt oder schließt die Haftung einer Partei gegenüber der anderen Partei aus (i) für alle vorsätzlich verursachten Schäden; (ii) für Personenschäden oder Todesfälle, die vorsätzlich, grob oder leicht fahrlässig durch die andere Partei verursacht wurden; (iii) für arglistiges Handeln; (iv) für jegliche Haftung, die nach Datenschutzgesetzen und anderem, zwingend anwendbarem, geltendem Recht nicht beschränkt oder ausgeschlossen werden kann; oder (v) gegenüber Betroffenen Personen oder zuständigen Datenschutzaufsichtsbehörden, die aufgrund von Datenschutzgesetzen nicht eingeschränkt werden kann.

b. Vorbehaltlich Abschnitt a. haftet jede Partei bei leicht fahrlässiger Verletzung einer wesentlichen Vertragspflicht (wobei sich der Begriff "wesentliche Vertragspflicht" abstrakt auf eine Verpflichtung bezieht, deren Erfüllung wesentlich ist für die ordnungsgemäße Erfüllung dieser ADV in Bezug auf die Verarbeitung Personenbezogener Daten und auf deren Einhaltung die andere Partei regelmäßig vertrauen kann) für Schäden hinsichtlich der Vereinbarung in Höhe des typischerweise vorhersehbaren Schadens. Die Höhe aller nach Satz 1 typischerweise vorhersehbaren Schäden ist auf eine Million Dollar (1.000.000 US-Dollar) begrenzt. Diese Haftungsbeschränkung gilt insgesamt und nicht pro Vorfall.

c. Vorbehaltlich der vorstehenden Abschnitte a. und b. ist jede weitere Haftung für beide Parteien - gleich aus welchem Rechtsgrund - ausgeschlossen. Insbesondere ist die Haftung ausgeschlossen für jegliche: (i) speziellen, zufälligen, indirekten Schäden oder Folgeschäden; (ii) entgangenen Gewinn, Umsatzverluste, entgangene Geschäftsabschlüsse, nicht realisierte Einsparungen, Nutzungsausfall oder entgangene Nutzungen, Verluste von Goodwill oder Rufschäden; (iii) verloren gegangene oder beschädigte Daten; oder (iv) vergeblichen Aufwendungen.

d. Sofern eine Verletzung des Schutzes Personenbezogener Daten oder ein Verstoß gegen diese ADV auch einen Verstoß gegen Vertraulichkeits- oder Geheimhaltungspflichten in der Vereinbarung darstellt, gilt die Haftungsbeschränkung gemäß Abschnitt b.

12) ALLGEMEINE REGELUNGEN

a. Die Gültigkeit, Auslegung und Erfüllung dieser ADV unterliegen dem deutschen Recht. Die Parteien unterwerfen sich der Rechtsprechung der deutschen Gerichte. Das UN-Kaufrecht (Convention on Contracts for the International Sale of Goods) findet keine Anwendung.

b. Niemand anderes als eine Partei dieser ADV, ihre Nachfolger und zugelassenen Abtretungsempfänger hat das Recht, eine der Bestimmungen dieser ADV durchzusetzen.

c. Diese ADV wird zum Datum des Inkrafttretens wirksam und bleibt für die Laufzeit der Vereinbarung, oder solange eine Verarbeitung der Personenbezogenen Ddaten des Kunden stattfindet, in Kraft.

d. Der Kunde muss seine E-Mail-Benachrichtigungen an privacy@cisco.com, mit privacy-germany@cisco.com in Kopie, senden. Cisco verwendet die in Ziffer 9 a) dieser ADV angegebene E-Mail-Adresse des Kunden für E-Mail-Benachrichtigungen. Die Parteien vereinbaren, dass eine Kündigung dieser ADV nur schriftlich per Brief möglich ist. Für diesen Brief sind die auf der ersten Seite dieser ADV angegebenen Adressen der Parteien mit Adressat „Rechtsabteilung“ zu verwenden.

Die Parteien veranlassen die Ausfertigung dieser ADV durch die Unterzeichnung ihrer zur Unterzeichnung autorisierten Vertreter.

Freie Universität Berlin
Die Kanzlerin
Kaiserswerther Straße 16-18
14195 Berlin

("**Kunde**")	("**Cisco**")
Unterschrift	Unterschrift
Name: Dr. Andrea Bör, Kanzlerin	Name: [redacted]
Datum: 10.02.2021	Datum: 8 February 2021

APPROVED BY LEGAL

CISCO
Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom

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.

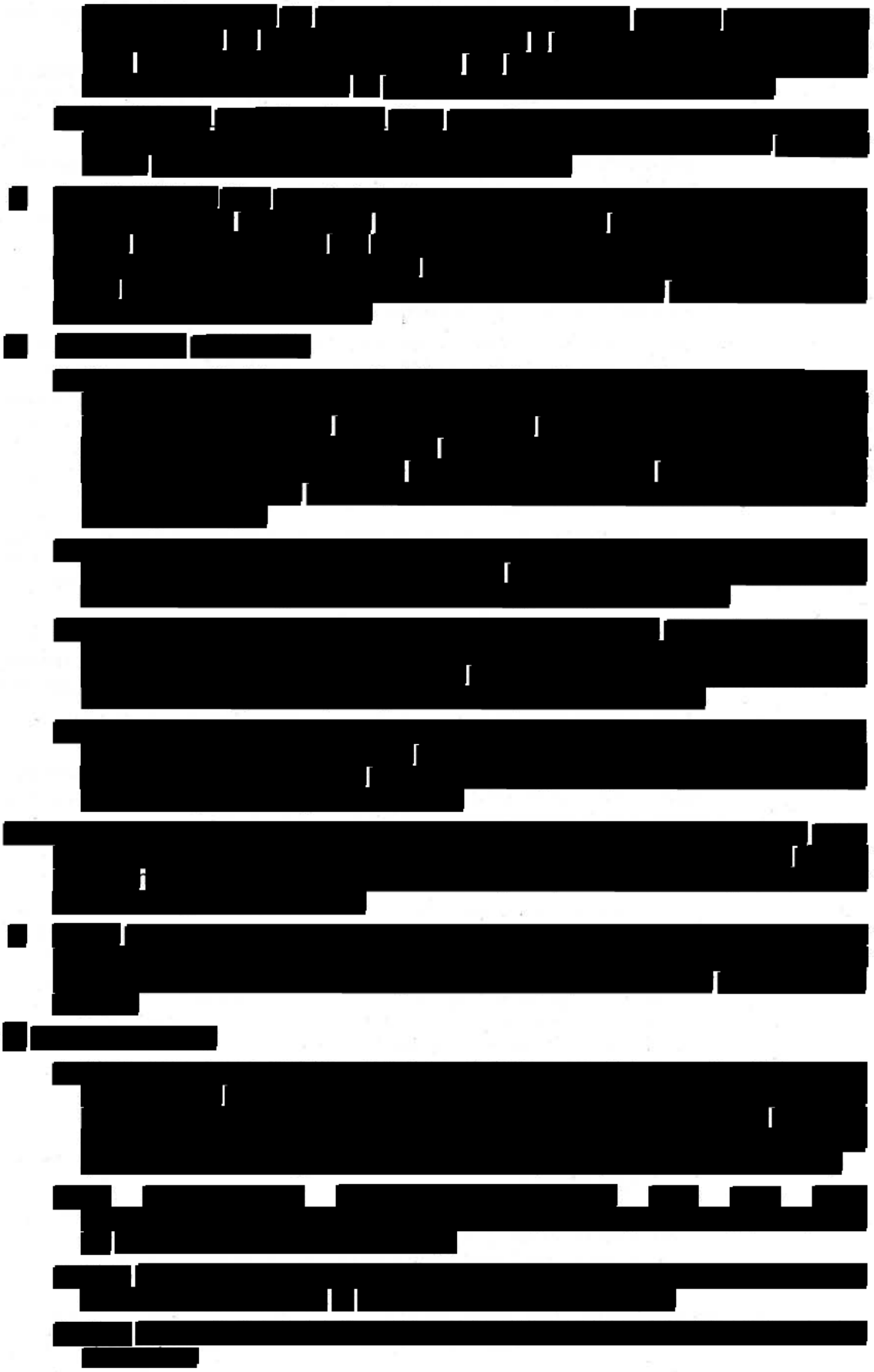
e. **Überprüfung der technischen Compliance.** Cisco muss seine Informationssysteme regelmäßig auf Übereinstimmung mit den Richtlinien und Standards von Cisco in Bezug auf Informationssicherheit überprüfen.

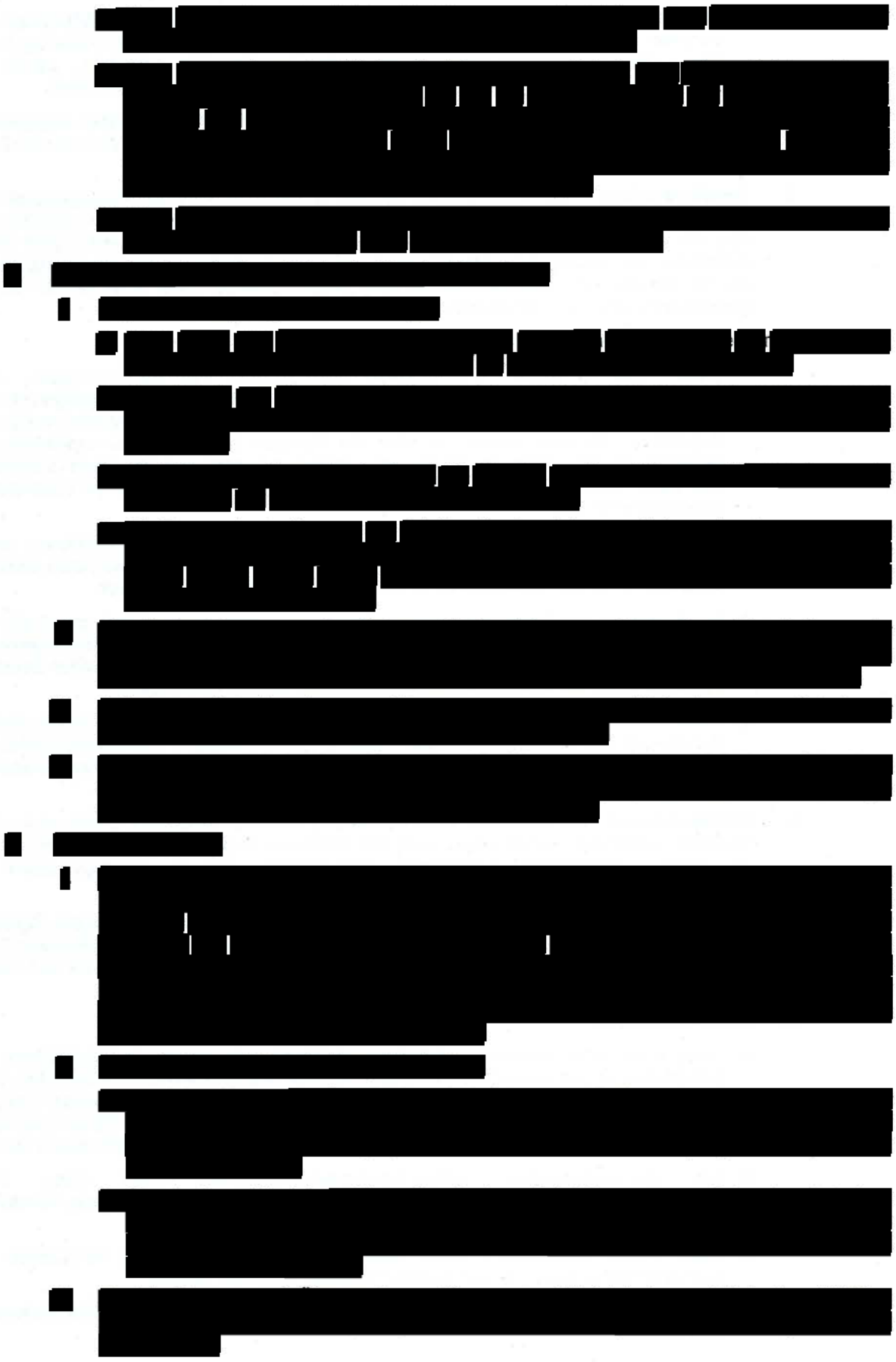
f. **Informationsbezogenes Risikomanagement („IRM").** Cisco muss einen angemessenen, im Einklang mit anwendbaren vertraglichen und rechtlichen Verpflichtungen stehenden Risikomanagementprozess in Bezug auf die Informationen implementieren und nutzen, um Risiken einzugrenzen, zu bewerten, auf sie zu 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.

4) Technische und organisatorische Sicherheitsmaßnahmen

[redacted]

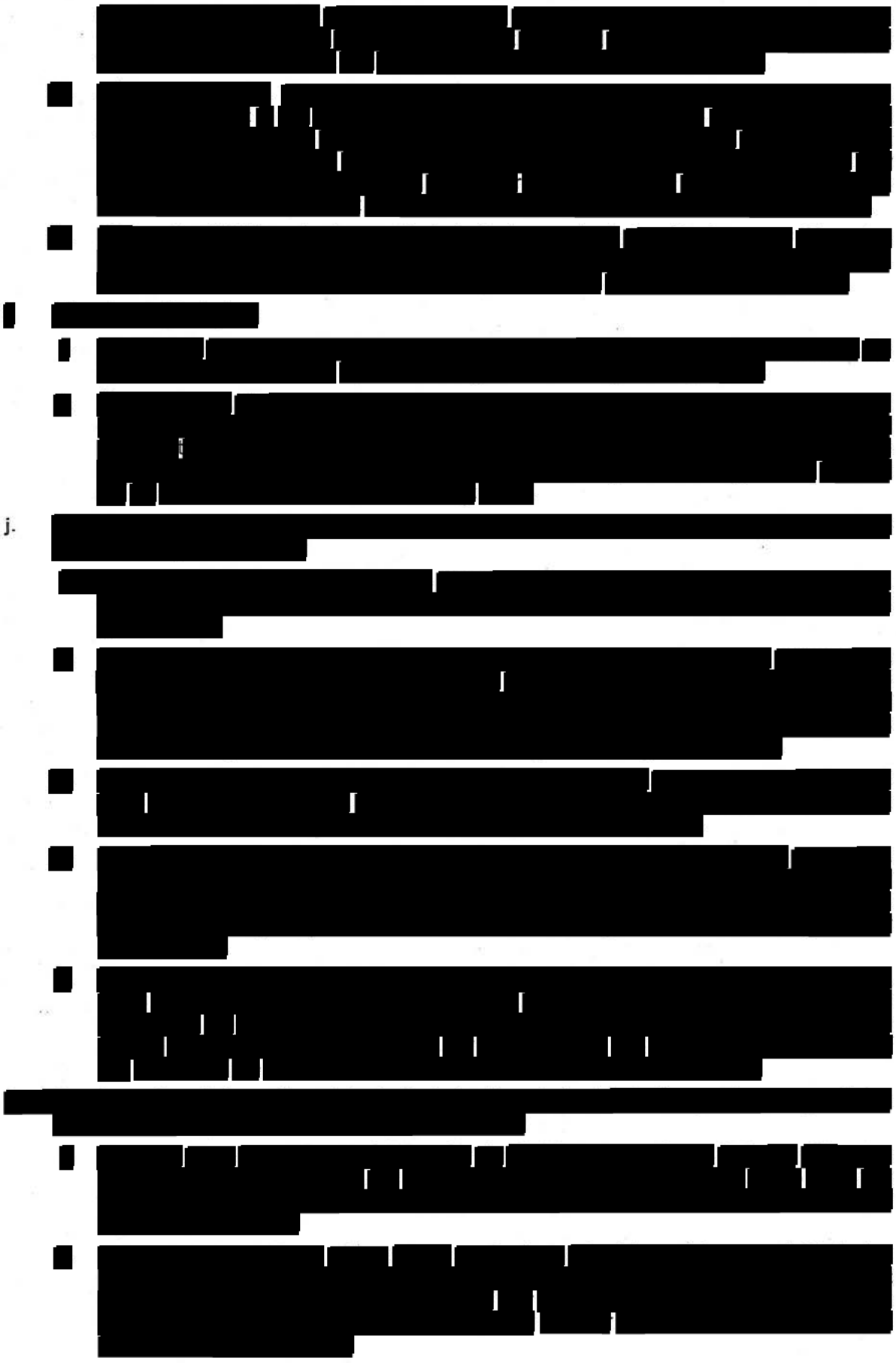




f. [redacted]

g. [redacted]

[redacted]



j.

ANLAGE B

BESCHREIBUNG DER VERARBEITUNG

Diese Anlage B beschreibt den Zweck, den Umfang, die Kategorien der Personenbezogenen Daten und die Betroffene Personen, die von einer Verarbeitung gemäß Art. 28 DSGVO betroffen sind.

Anhang 1 zu dieser Anlage B enthält die genaue Beschreibung der Verarbeitung je Produkt und/ oder Service.

ANHANG 1 ZU ANLAGE B

TEIL 1 – CISCO WEBEX MEETINGS

Dieser Anhang 1 zu Anlage B „Teil 1 – Cisco Webex Meetings" spezifiziert den Gegenstand der Verarbeitung. Cisco Webex-Meetings wird in diesem Anhang 1 zu Anlage B als "Service" oder "Webex Meetings" bezeichnet.

Gegenstand der Verarbeitung

Webex Meetings ist eine cloudbasierte Web- und Videokonferenzlösung, die Cisco dem Kunden zur Verfügung stellt, der sie für die Verwendung durch autorisierte Benutzer erwirbt. Webex Meetings ermöglicht Mitarbeitern und virtuelle Teams in Echtzeit von jedem Ort und zu jeder Zeit auf jedem mobilen Gerät oder Videosystem zusammenarbeiten, als würden sie im selben Raum sitzen. Die Lösungen umfassen Besprechungen, Veranstaltungen, Schulungen und Support-Services.

Mit Webex Meetings können Benutzer sofort eine Verbindung herstellen, die so persönlich ist wie eine Besprechung in Person. Der Besprechungsleiter hat die Möglichkeit, Besprechungen aufzuzeichnen, und alle Benutzer haben die Möglichkeit, während und außerhalb von Besprechungen gemeinsam genutzte Dateien hochzuladen und zu speichern. Wenn der Besprechungsleiter entscheidet, den Besprechungsinhalt nicht beizubehalten, wird er sofort nach Abschluss der Besprechung von der Cisco Webex-Plattform entfernt.

Wenn Benutzer an Besprechungen teilnehmen, die von Benutzern in anderen Unternehmen veranstaltet werden, kontrolliert der Besprechungsleiter alle während der Besprechung freigegebenen Besprechungsaufzeichnungen oder -dateien, die seinen Unternehmensrichtlinien in Bezug auf Zugriff, Verwendung, Überwachung, Löschen, Aufbewahrung und Export von Informationen unterliegen. Cisco hat keinen Einfluss darauf und ist nicht verantwortlich oder haftbar für die Vertraulichkeit von Informationen, die der Kunde mit anderen geteilt hat. Auch nachdem der Kunde Informationen von der Webex-Plattform entfernt hat, können Kopien dieser Informationen an anderer Stelle angezeigt werden, sofern sie mit anderen Besprechungsteilnehmern geteilt wurden.

Die folgenden Kategorien von Personenbezogenen Daten können für den spezifizierten Verarbeitungszweck verarbeitet werden:

Webex Suite = Webex Meetings, Webex Events, Webex Support und Webex Training:

Kategorie der Personenbezogenen Daten	**Arten von Personenbezogenen Daten**	**Zweck der Verarbeitung**
Nutzer informationen	• Name • E-Mail-Adresse • Passwort • IP Adresse • Browser • Telefonnummer (Angabe freiwillig) • Postanschrift (Angabe freiwillig) • Region (geografisch) • Avatar (Angabe freiwillig) • Abrechnungsinformationen • Benutzerinformationen die in dem Active Directory des Kunden enthalten sind (sofern synchronisiert) • Unique User ID ("UUID")	• Zurverfügungstellung des Service • Registrierung für den Service • Anzeigen der Avatar-Identität des Kundenbenutzers für andere Benutzer • Teilnahme an Verbesserungen des Service • Bereitstellung von Unterstützung • Benachrichtigung über Funktionen und Updates für der Service • Authentifizierung und Autorisierung für den Kontozugriff • Anzeigen von Directory Informationen für andere Benutzer • Verwendung der schrittweise Anleitungen zur Verwendung von Webex online über WalkMe (optional)
Host- und Nutzungsinformationen	• IP Adresse • Benutzeragentenkennung • Hardwaretyp	• Zurverfügungstellung des Service

	• Betriebssystem Typ, Version • Client-Version • Browser • IP Adressen entlang des Netzwerkpfads • MAC-Adresse des Endpunkts (sofern zutreffend) • Serviceversion • Ergriffene Maßnahmen • Region (geografisch) • Informationen zur Besprechungssitzung (Titel, Datum und Uhrzeit, Häufigkeit, durchschnittliche und tatsächliche Dauer, Anzahl, Qualität, Netzwerkaktivität und Netzwerkkonnektivität) • Anzahl der Meetings • Anzahl der Screen-Sharing- und Non-Screen-Sharing-Sitzungen • Zahl der Teilnehmer • Meeting Host Information: Host Name und ID, Meeting Site URL, Meeting Start/End Zeitpunkt • Bildschirmauflösung • Einwahlmethode • Informationen zu Leistung, Fehlerbehebung und Diagnose • Teilnehmerinformationen, einschließlich E-Mail-Adresse, IP Adresse, Benutzername, Telefonnummer, Raumgeräteinformation	• Zum genaueren Verständnis für den Kunden, wie der Service verwendet wird • Diagnostik technischer Probleme • Zurverfügungstellung von Analysen und statistische Analysen in aggregierter Form, um die technische Leistung des Service zu verbessern • Antworten auf Kundenanfragen • • Verbesserungen des Service
Benutzergenerierte Informationen	• Besprechungs- und Anrufaufzeichnungen • Hochgeladene Dateien	• Zurverfügungstellung des Services. • Besprechungsaufzeichnung und gemeinsame Nutzung von hochgeladenen Dateien können optional genutzt werden.
Webex Analysedaten	• Registrierungsinformationen • Host- und Nutzungsinformationen	• Bereitstellung von Nutzungstrends und wertvollen Erkenntnissen zur Unterstützung von Strategien zur Förderung und Optimierung der Akzeptanz in Teams • Bereitstellung erweiterter Analysefunktionen und Berichte

Betroffene Personen

Die verarbeiteten Personenbezogenen Daten können folgende Kategorien Betroffener Personen betreffen:

Mitarbeiter des Unternehmens oder des Kunden, Teilnehmer. Personen, deren Daten Gegenstand der Kommiunikation sind.

Grenzüberschreitende Übermittlung

Der Service nutzt seine eigenen Rechenzentren, um weltweit zur Verfügung zu stehen. Die Rechenzentren von Webex Meetings befinden sich derzeit in folgenden Ländern:

Kategorie der Personenbezogenen Daten	**Arten von Personenbezogenen Daten**	**Standort der Cisco Rechenzentren**
Benutzergenerierte Informationen	Wie in der Tabelle oben beschrieben. Benutzergenerierte Informationen werden in dem Rechenzentrum gespeichert, dass bei der Bestellung des Service ausgewählt worden ist.	EU, Vereinigtes Königreich
Webex Analysedaten (Berichte)	Wie in der Tabelle oben beschrieben.	USA

Ein Internet Point of Presence (iPOP) wird verwendet, um den Datenverkehr geografisch von nahegelegenen Gebieten zu einem Cisco Rechenzentrumstandort zu leiten. Es ist beabsichtigt, den Webex Meeting-Verkehr durch die Cisco-Infrastruktur zu leiten und die Leistung zu verbessern. Daten, die über diese iPOPs geleitet werden, bleiben verschlüsselt und werden nicht gespeichert. Weitere Details finden Sie in den Privacy Data Sheet(s).

Unterauftragsverarbeiter

Cisco gibt Registrierungs-, Host- und / oder Nutzungsinformationen an Unterauftragsverarbeiter weiter, um bei der Bereitstellung und Verbesserung des Service zu unterstützen. Der gesamte Informationsaustausch erfolgt im Einklang mit dieser ADV, um sicherzustellen, dass die Unterauftragsverarbeiter das gleiche Maß an Datenschutz und Informationssicherheit bieten können, das Sie von Cisco erwarten können.

Im Folgenden werden die Unterauftragsverarbeiter dargestellt:

Unterauftrags-verarbeiter	Personenbezogene Daten	(Teil-) Leistungsgegenstand der Verarbeitung im Rahmen der Vereinbarung	Standort
Akamai Technologies, Inc.* 150 Broadway Cambridge, MA 02142 USA * Die Bereitstellung von CDN-Diensten kann auf Kundenwunsch abgeschaltet werden.	IP-Adressen, Browser und geografische Region	Akamai wird als Content Delivery Network (CDN)-Dienstleister für statische Inhalte eingesetzt.	Weltweit
Amazon Web Services, Inc. (AWS) 410 Terry Avenue North, Seattle, WA 98109-5210, USA	Begrenzte Host- und Benutzerinformationen, die den Medienverkehr erfüllen.	Die AWS-Cloud-Infrastruktur wird zum Hosten des Webex-Signalisierungsdienstes verwendet, der Informationen zum Lebenszyklus von Besprechungen in Echtzeit verarbeitet, z. B. UUID´s von Besprechungsteilnehmern, Start- und Endzeiten von Besprechungen. Die Daten werden innerhalb von 15 Tagen nach dem Meeting gelöscht (Standortzuordnungen zur Webex-Rechenzentrumszuweisung des Kunden). Die AWS-Cloud-Infrastruktur wird zudem Hosten von Webex Medienknoten verwendet, die Echtzeitbesprechungsdaten wie VoIP, Video und Daten mit hoher Bitrate verarbeiten können. Diese Informationen werden nach Beendigung Ihrer Besprechung nicht mehr in AWS gespeichert.	Deutschland Niederlande Vereinigtes Königreich USA Brasilien Australien Japan Singapur
WalkMe, Inc.* 71 Stevenson St floor 20, San Francisco, California, 94105, USA * * Das Feature wird für Unternehmensstandorte im Juni 2020 aktiviert. Kunden können es jederzeit deaktivieren. Das Feature ist derzeit für Webex-Sites außerhalb des Unternehmens aktiviert.	Verarbeitung von UUID und Benutzerregion	Das WalkMe Feature bietet dem Benutzer eine schrittweise Anleitung. Der Verantwortliche (jeder Cisco Kunde) kann dieses Feature zu jeder Zeit abstellen lassen.	Weltweit

ANLAGE C

STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)

Zum Zwecke von Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist, gilt Nachfolgendes.

Für die Zwecke dieser Anlage C gilt:

„**Datenexporteur**" bezeichnet den Kunden, der gegebenenfalls als Datenexporteur im Namen seiner Kunden im EWR oder in der Schweiz agiert,

und

„**Datenimporteur**" bezeichnet Cisco.

die „**Partei**", wenn eine dieser Organisationen gemeint ist, die „**Parteien**", wenn beide gemeint sind.

The Parteien vereinbaren folgende Vertragsklauseln („Klauseln"), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1);

b) der „Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter" ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiter des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht" bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen" sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2

Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3

Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur nieder- gelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Stan- des der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durch- geführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.
Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7

Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder
b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11

Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss (1). Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht

mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j über- mittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klauseln 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

Im Auftrag des Datenexporteurs: **Freie Universität Berlin**

Name (vollständig ausgeschrieben): **Dr. Andrea Bör**
Kanzlerin

Adresse: Kaiserswerther Str. 16/18, 14195 Berlin, Deutschland

Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift .....

10.02.2021

Im Auftrag des Datenimporteurs: **Cisco Systems, Inc.**

Name (vollständig ausgeschrieben): [redacted]

Position:

Adresse: 170 West Tasman Dr., San Jose, CA 95134, USA

Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift [redacted]

8 February 2021 APPROVED BY LEGAL

Im Auftrag des Datenimporteurs: **Cisco International Limited**

Name (vollständig ausgeschrieben): [redacted]

Position:

Adresse: 9-11 New Square, Bedfont Lakes, Feltham,
Middlesex TW14 8HA, United Kingdom

Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift [redacted]

8 February 2021 APPROVED BY LEGAL

CISCO
Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom

ANHANG 1 ZU ANLAGE C STANDARDVERTRAGSKLAUSELN

"TEIL 1 – CISCO WEBEX MEETINGS"

Dieser Anhang 1 zu Anlage C Standardvertragsklauseln „Teil 1 – Cisco Webex Meetings" ist Bestandteil der Standardvertragsklauseln. Cisco Webex-Meetings wird in diesem Anhang 1 zu Anlage C als "Service" oder "Webex Meetings" bezeichnet.

Datenexporteur

Datenexporteur ist der Kunde, der gegebenenfalls in eigenem Namen oder im Namen eines Nutzers als Datenexporteur agiert. Zu den für die Übermittlung relevanten Aktivitäten gehört die Erbringung von Leistungen für den Kunden und dessen Nutzer.

Datenimporteur

Datenimporteur ist Cisco. Zu den für die Übermittlung relevanten Aktivitäten gehört die Erbringung von Leistungen für den Kunden und dessen Kunden.

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien Betroffener Personen:

Wie in Anhang 1 zu Anlage B, Teil 1 - Cisco Webex Meetings aufgeführt.

Kategorien von Daten

Die übermittelten personenbezogenen Daten gehören zu den folgenden Datenkategorien:

(1) Nutzerinformationen
(2) Host- und Nutzungsinformationen
(3) Benutzergenerierte Informationen
(4) Webex Analysedaten

Alle Details zu (1) – (4) sind in Anhang 1 zu Anlage B, Teil 1 - Cisco Webex Meetings aufgeführt.

Besondere Datenkategorien

Die übermittelten Personenbezogenen Daten können in die folgenden besonderen Kategorien von Daten fallen:

Nicht anwendbar.

Datenverarbeitung

Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

Die personenbezogenen Daten werden zu dem beschriebenen Zweck und wie in Anhang 1 zu Anlage B, Teil 1 - Cisco Webex Meetings beschrieben, verarbeitet.

ANHANG 2 ZU ANLAGE C STANDARDVERTRAGSKLAUSELN

Anhang 2 zu Anlage C Standardvertragskauseln sind die Maßnahmen zur Informationssicherheit, wie in Anlage A Informationssicherheit beschrieben.