Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin

An die
Kanzlerin der Freien Universität Berlin
Frau Dr.-Ing. Andrea Bör
Kaiserswerther Str. 16-18
14195 Berlin

Vorab per E-Mail:
rechtsamt@fu-berlin.de

Geschäftszeichen: (bitte angeben) 51.1359.10
Abteilung: I B
Bearbeiter(in): [redacted]
Telefon: 030 13889-0
Durchwahl-Nr.: [redacted]

Datum: 16. November 2021

Einsatz von Cisco Webex an der Freien Universität Berlin

Sehr geehrte Frau Dr. Bör,

ich nehme Bezug auf die bisher geführte Kommunikation über die Nutzung des Videokonferenz- und Kommunikationsdienstes Cisco Webex in der Cloud-Version durch die Freie Universität Berlin.

Meine Mitarbeiterinnen und Mitarbeiter haben angesichts der Wünsche mehrerer Verwaltungen, die Cloud-Lösung von Cisco Webex Meetings einzusetzen, in den letzten Monaten erhebliche Anstrengungen unternommen, um im Dialog mit Cisco, der Senatskanzlei und der zentralen IKT-Steuerung eine Lösung zu finden, die Cloud-Lösung von Cisco Webex Meetings rechtskonform einsetzen zu können. All diese Versuche sind leider gescheitert. Die von Cisco zugesagten Änderungen in Richtung einer Verringerung der Datenschutzverstöße sind bis heute im Wesentlichen nicht umgesetzt und wir haben nicht einmal die seitens Cisco zugesagten Informationen zum Stand der Umsetzung erhalten. Insbesondere besteht zwar offensichtlich mittlerweile ein Rechenzentrum in Frankfurt am Main, das Sie auch nutzen – doch leider wird hierüber nur ein Teil des Datenverkehrs abgewickelt, und zwar offenbar derjenige, der zuvor über das Rechenzentrum in Amsterdam abgewickelt wurde. Die rechtswidrigen Übermittlungen personenbezogener Daten in die USA und die bereits auf erster Stufe rechtswidrigen Datenverarbeitungen hat Cisco – soweit für meine Mitarbeiter*innen von außen erkennbar – nicht beendet. Ebenso bestehen die Probleme des nicht gesetzeskonformen Auftragsverarbeitungsvertrags und der nach europäischem Recht unzulässigen Zugriffsbefugnisse US-amerikanischer Behörden fort. Darüber hinaus werden bei der Leistungserbringung auch weiterhin nicht vertraglich zugelassene Subunternehmer eingesetzt.

Die von Ihnen unter https://fu-berlin.webex.com genutzte Lösung lässt sich daher derzeit nicht datenschutzkonform nutzen.

Um zu eruieren, ob und ggf. über welchen Zeitraum eine fortgesetzte Nutzung des Dienstes tolerierbar erscheint, ist zu klären, ob seitens der FU bestimmte technische und organisatorische Maßnahmen getroffen werden können, die die Verletzung der Grundrechte der betroffenen Personen entscheidend verringern.

Dies beinhaltet mehrere Aspekte:

- Die Inhalte der Kommunikation müssen Ende-zu-Ende-verschlüsselt werden. Cisco Webex Meetings sieht hierfür eine optional aktivierbare Funktion vor. Bei einer Kurzprüfung durch mein Haus haben sich jedenfalls keine offensichtlichen Schwächen gezeigt, die die Ende-zu-Ende-Verschlüsselung als offensichtlich ungeeignet erscheinen lassen würden.

  Ich muss allerdings darauf hinweisen, dass bei Aktivierung der Ende-zu-Ende-Verschlüsselung eine Teilnahme an den Videokonferenzen nur noch mittels der Cisco-App möglich ist. Insbesondere ist eine Einwahl per Telefon, Web-Browser oder SIP nicht mehr möglich. Auch die Linux-Version der App ermöglicht laut Cisco-Webseite keine Nutzung von Ende-zu-Ende-Verschlüsselung.

  Da laut den auf verschiedenen FU-WWW-Seiten veröffentlichten Informationen auch eine Teilnahme per Browser möglich ist, kann somit Ihre Aussage in Ihrer Antwort auf Frage 12.b und in verschiedenen Dokumenten einschließlich der Informationen nach Art. 13 DS-GVO nicht richtig sein, dass Sie Webex mit Ende-zu-Ende-Verschlüsselung nutzen.

- Die im Rahmen der Nutzung des Dienstes anfallenden technischen Daten müssen vor Offenlegung an Cisco anonymisiert oder so pseudonymisiert werden, dass Cisco und die US-Behörden das Pseudonym nicht auf einzelne Personen oder kleine Gruppen zurückführen können. Dies betrifft zuvörderst die IP-Adresse, die für US-Behörden nur ein äußerst schwaches Pseudonym darstellt. Hierfür könnten Sie beispielsweise allen Teilnehmenden ein VPN zur Teilnahme an Webex bereitstellen oder Webex nur über eine Proxy-Lösung zugänglich machen.

Soweit die verwendete App auch weitere personenbezogene Daten sammelt, etwa Hardware-Adressen, und dies nicht – sei es durch Einstellungen, sei es durch Blockade des Datenverkehrs – unterbunden werden kann, sind auch diese technisch zu verbergen. Hierzu könnte die Nutzung virtueller Maschinen erforderlich werden. Alternativ könnten Sie den Teilnehmenden gesonderte Hardware ausschließlich für den Zweck der Nutzung des FU-Cisco-Webex-Dienstes bereitstellen.

- Auch die Daten der Teilnehmenden – etwa die angezeigten Namen und die Daten der einladenden Personen – müssen für Cisco und US-Behörden unauflösbar pseudonymisiert werden. Dies kann beispielsweise dadurch erfolgen, dass für die Organisation der Videokonferenzen zentrale Accounts genutzt werden oder pseudonyme Kennungen, deren Zuordnung zu den tatsächlichen Nutzer*innen nur der FU bekannt ist. Es ist im Fall der Nutzung von Pseudonymen allerdings zu beachten, dass die Zuordnung auch nicht anderweitig für die US-Behörden auflösbar sein darf, etwa durch Versendung von E-Mails, die erkennen lassen, dass eine bestimmte Person eine bestimmte Videokonferenz einberufen hat. Insofern empfiehlt sich für die Anlage von Videokonferenzen die Nutzung zentraler Accounts. Die Nutzung von Klardaten wie bisher durch Anbindung an die FU-Systeme erscheint nicht tolerierbar.

  In diesem Zusammenhang gestatte ich mir den Hinweis, dass die von Ihnen in Ihrer Antwort auf Frage 16 genannte Rechtsgrundlage für die Verarbeitung von Namen und E-Mail-Adressen der Teilnehmenden nicht tragfähig erscheint. Eine Erforderlichkeit ist nicht ersichtlich, wie Sie durch den Hinweis auf die Möglichkeit der Nutzung eines Pseudonyms selbst zugestehen. In Ihrer Datenschutzerklärung dagegen bezeichnen Sie die Angabe von Vorname, Nachname und E-Mail-Adresse mehrfach als zwingend; der später erfolgende Hinweis auf die Möglichkeit der Angabe eines Pseudonyms für die Teilnahme an Online-Meetings ist verwirrend. Sie müssten daher bitte umgehend die Erhebung der E-Mail-Adresse deaktivieren und unübersehbar klarstellen, dass als Name bei der Teilnahme nur ein Pseudonym angegeben werden sollte, da dieses US-Behörden zur Kenntnis gelangen und von diesen nach dem Maßstab europäischer Grundrechte unrechtmäßig genutzt werden kann.

Ich bitte um zeitnahe Mitteilung, in welcher Weise Sie die aufgezeigten Änderungen umsetzen werden und um Übersendung eines konkreten Zeitplans hierfür. Gern bin ich bereit, mit Ihnen dann ggfs. in Gespräche einzutreten, wie lange – immer vorbehaltlich eines konkreten Handlungsbedarfs angesichts von Beschwerden – der bestehende rechtswidrige Zustand noch geduldet werden kann.

Ich schlage vor, dass Sie auf Arbeitsebene Kontakt mit meinem Referatsleiter [redacted], aufnehmen, was die konkrete Umsetzung und den Zeitplan angeht.

Darüber hinaus übersende ich Ihnen in der Anlage eine Liste mit möglichen Änderungen zur Verbesserung des Datenschutzes beim Einsatz von Cisco Webex Meetings. Teil 1 dieser Liste ist ohne Weiteres umsetzbar. Ich bitte Sie, dies umgehend zu tun und mir die Umsetzung anhand von Screenshots u. Ä. nachzuweisen. Teil 2 erfordert zunächst Prüfungen. Ich bitte Sie, diese umgehend vorzunehmen und mir die Ergebnisse im Detail mitzuteilen.

Hinsichtlich Ihres Einsatzes von Webex Events, Webex Training und Webex Teams weise ich darauf hin, dass Sie hierfür keinen Auftragsverarbeitungsvertrag mit Cisco abgeschlossen haben. Die derzeitige Nutzung ist daher rechtswidrig. Grund dafür, dass diese Dienste nicht von dem von Ihnen abgeschlossenen Auftragsverarbeitungsvertrag umfasst sind, ist, dass der Muster-Auftragsverarbeitungsvertrag von Cisco im Austausch mit meinen Mitarbeiter*innen erheblich verbessert wurde, allerdings die Beteiligten keine Möglichkeit gesehen haben, die Nutzung dieser Dienste rechtmäßig zu gestalten. Daher wurden diese Dienste von vornherein aus dem Vertrag entfernt.

Sollten Sie diese Dienste weiterhin nutzen wollen, bitte ich Sie, umgehend die in diesem Zusammenhang erfolgenden Datenverarbeitungen zu überprüfen, auch im Hinblick auf die oben genannten Anforderungen für eine Duldung, und einen umfassenden Auftragsverarbeitungsvertrag abzuschließen. Bitte teilen Sie mir auch insoweit mit, welche Maßnahmen Sie mit welchen Ergebnissen ergriffen haben.

Auf die Hinweise von Frau Smoltczyk im Schreiben vom 9. Juni 2021 nehme ich Bezug.

Mit freundlichen Grüßen

[redacted]

Dienststellenleiter (Komm.)

Anlage: Mögliche datenschutzrechtliche Verbesserungen

Teil 1: Änderungen an den Einstellungen von Cisco Webex Cloud

1. Stellen Sie sicher, dass die Option der „Global Distributed Meetings“ (GDM) abgeschaltet ist. Hierbei handelt es sich um eine weltweit verteilte Fail-Over-Konstruktion, die vorsieht, dass für Vermittlung und Durchführung der Videokonferenz-Kommunikation je nach Auslastung und Funktionsfähigkeit unterschiedliche Rechenzentren innerhalb und außerhalb der EU eingesetzt werden. Hierbei kommt es ggf. zu einem vertrags- und rechtswidrigen Datenexport. Hierzu muss ein Op-Request bei Cisco erfolgen.

2. Stellen Sie sicher, dass die kund*innenspezifische WWW-Seite für die Videokonferenzen keine Inhalte von anderen Servern lädt, die entweder außerhalb der EU/des EWR lokalisiert sind oder von nicht autorisierten Sub-Auftragsverarbeitern betrieben werden. Dies betrifft beispielsweise den Server akamaicdn.webex.com. Nach Angaben von Cisco ist eine entsprechende Konfiguration des Accounts möglich.

3. Um den Anforderungen an datenschutzfreundliche Voreinstellungen gerecht zu werden, sind ferner einige Einstellungen im Control Hub notwendig. Diese sind wie folgt:
   - Der „Lesezugriff für den Support von Cisco und Cisco-Partnern auf die Organisation“ ist zu deaktivieren.
   - Das „Crash-Reporting“ ist zu deaktivieren.
   - Die „Gesichtserkennung für Name-Labels“ ist zu deaktivieren.
   - Unter „Archivierung“ sind die Löschfristen für gespeicherte Daten einzustellen, um den Anforderungen an Datenminimierung und Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. c und e DS-GVO gerecht zu werden und den Löschpflichten nach Art. 17 DS-GVO nachzukommen.

4. Bei den „Site-Optionen“ sind folgende Einstellungen umzusetzen:
   - Die „Unterstützung der Richtlinie zur automatischen Löschung von Aufzeichnungen“ ist zu aktivieren.
   - Die „Aufbewahrungsdauer für Aufzeichnungen in Tagen“ ist auf null zu setzen.
   - Die „Lokale Aufzeichnung für Webex-Meetings, -Events, -Schulungssitzungen und Webex Teams-Meetings“ ist zu deaktivieren.

- Für entsperrte Meetings ist die Option „Gäste warten in der Lobby, bis sie vom Gastgeber hereingelassen werden“ zu aktivieren, es sei denn, die Veranstaltung ist öffentlich. Dies bezieht sich sowohl auf Webex Meetings als auch auf persönliche Räume.
- Die Option „Erfordert E-Mail-Adresse des Teilnehmers“ ist zu deaktivieren.
- Die Funktion der „Nachverfolgungscodes“ zur Erfassung des Nutzerverhaltens der Teilnehmenden ist zu deaktivieren.

Teil 2: Prüfungen und Konsequenzen

1. Cisco bietet verschiedene Client-Apps an. Mindestens eine davon verlangt zwingend die Zustimmung zur Verarbeitung personenbezogener Daten durch Cisco zu eigenen Zwecken. Bitte prüfen Sie, ob dies bei den von der FU empfohlenen/verlinkten/genutzten Apps ebenso der Fall ist. Betroffene Apps dürfen nicht genutzt werden.

2. Bei der Nutzung von Cisco Webex Meetings werden personenbezogene Daten unzulässig an verschiedene Server übertragen, insbesondere auch detaillierte Daten zur Nutzung in die USA. Bitte prüfen Sie, ob diese Datenflüsse für ein Funktionieren der Videokonferenzlösung zwingend technisch erforderlich sind (wohl jedenfalls überwiegend nicht). Blockieren Sie alle Servernamen (FQDN), an die unzulässig Daten abfließen und die nicht technisch erforderlich sind, auf allen Clients bzw. auf VPN-/Proxy-Ebene, etwa durch Firewall-Regeln, hosts-Einträge, Ausfiltern aus dem Datenverkehr o. Ä.