Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Friedrichstr. 219
10969 Berlin
Besuchereingang:
Puttkamer Str. 16-18

Telefon: (030) 13889-0
Telefax: (030) 215 50 50
mailbox@datenschutz-berlin.de

Sprechzeiten

tgl. 10-15 Uhr, Do. 10-18 Uhr
(oder nach Vereinbarung)

Erreichbarkeit

U6: Kochstr.
Bus: M29, 248

Internet

https://datenschutz-berlin.de

Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen

Die Vorsorgemaßnahmen zur Eindämmung der Corona-Pandemie führen in nahezu allen Bereichen des täglichen Lebens zu Einschränkungen. Um physische Nähe zwischen Menschen möglichst zu vermeiden, gehört hierzu in sehr vielen Fällen, dass berufliche Kontakte nicht mehr persönlich, sondern über das Netz gehalten werden. Wenn mehr als zwei, drei Personen eine gemeinsame Unterredung führen wollen, werden nun Telefon- und Videokonferenzen abgehalten. Viele Unternehmen und Behörden suchen gut funktionierende Angebote für deren Durchführung und stellen zunächst die Prüfung zurück, ob sie auch datenschutzgerecht in Anspruch genommen werden können.

Mit diesem Text möchte die Berliner Beauftragte für Datenschutz und Informationsfreiheit den ihrer Aufsicht unterliegenden Unternehmen, Behörden und anderen Institutionen Hinweise zu den Anforderungen an die Nutzung von Videokonferenzsystemen geben und die Risiken beschreiben, die entstehen, wenn sie nicht eingehalten werden. Um diese Risiken zu vermeiden oder zumindest zu mindern und die datenschutzrechtlichen Vorgaben einzuhalten, sind die Verantwortlichen aufgerufen, kurzfristig eingesetzte, aber nicht datenschutzgerechte Lösungen sobald wie möglich durch datenschutzgerechte zu ersetzen bzw. entsprechend nachzubessern.

Personenbezogene Daten in Videokonferenzen

Personenbezogene Daten spielen bei der Durchführung von Videokonferenzen auf zwei Weisen eine Rolle: Erstens kann das gesprochene Wort selbst Informationen über einzelne Personen enthalten. Zweitens fallen bei der Durchführung einer Videokonferenz auch Daten über die Teilnehmerinnen und Teilnehmer an, d. h. ihre Kontaktdaten, ihre Namen sowie Angaben über Zeit und Ort ihrer Teilnahme an der Konferenz. Darunter sind auf jeden Fall Daten über Beschäftigte der Institution, die die Videokonferenz organisiert, und ggf. Daten über ihre Gesprächspartner/-innen, seien es Geschäftspartner/-innen, Mitarbeiter/-innen anderer Institutionen oder Privatpersonen.

Grundlegende Anforderungen und Empfehlungen

- Videotelefonie und Videokonferenzen sollen über verschlüsselte Kanäle abgewickelt werden. Dies betrifft sowohl die Vermittlung der Verbindungen als auch die Übertragung der Ton- und Bilddaten.
- Wenn Sie die Videokonferenzlösung nicht selbst sicher und mit angemessenem Aufwand betreiben können (was vorzuziehen wäre), dann können Sie einen zuverlässigen Videokonferenzdienst damit beauftragen. Voraussetzung ist, dass Sie einen Auftragsverarbeitungsvertrag

mit ihm schließen und der Betreiber keine Angaben über die Beschäftigten und deren Kommunikation oder die Nutzung der Software für eigene Zwecke verarbeitet oder an Dritte weitergibt.

Der Dienstleister sollte die Daten in der Europäischen Union, einem Land des Europäischen Wirtschaftsraums oder in einem als gleich sicher geltenden Land verarbeiten und auch dort seinen Sitz haben. Die Gleichwertigkeit stellt die Europäische Kommission fest (siehe https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de). Alternativ kann der Datenexport sich auf den Abschluss eines Vertrages stützen, dessen Text die von der EU-Kommission genehmigten Standardvertragsklauseln enthält (s. u.). Die Anforderung gilt auch für alle Unterauftragnehmer, die der Dienstleister seinerseits in Anspruch nimmt.

- Soweit nicht durch Verschlüsselung ausgeschlossen ist, dass die übermittelten Audio- und Videodaten durch den Anbieter zur Kenntnis genommen werden können, wird empfohlen, nur Anbieter in der Eueorpäischen Union oder dem Europäischen Wirtschaftsraum zu verwenden, wenn innerhalb der Videokonferenz sensible Daten besprochen werden sollen. Berufsgeheimnisträger dürfen nur Dienstleister einsetzen, die bei einem Vertraulichkeitsbruch strafrechtlich belangt werden können. Medizinische Leistungserbringer dürfen nur zertifizierte Dienstleister einsetzen, siehe https://www.kbv.de/html/videosprechstunde.php.

Risiken

Ein wesentliches Risiko besteht darin, dass bei der Videokonferenz unbefugt mitgehört oder die Inhalte aufgezeichnet und weiter ausgewertet werden, möglicherweise zum Nachteil der Personen, die an der Konferenz teilgenommen haben oder über die gesprochen wurde. Das Risiko ist am größten, wenn in dem Austausch sensible Themen angesprochen werden wie z. B. der Gesundheitszustand oder die politischen Auffassungen einer Person.

Dritte können versuchen, ein Gespräch auf dem Weg zwischen den Teilnehmenden und dem Betreiber des Angebots mitzuhören oder mitzuschneiden. Aber auch der Betreiber des Videokonferenzsystems selbst kann ein Interesse haben oder behördlich dazu verpflichtet sein, einen Mitschnitt anzufertigen, sei es, um lediglich die Qualität der Übertragung zu beurteilen, sei es, weil der Mitschnitt im Auftrag Dritter für deren Zwecke erfolgt.

Videokonferenzsysteme sind in der Regel so angelegt, dass bei dem Betreiberdienst die unverschlüsselten Bilder und Töne zusammenlaufen. Dadurch kann er den Strom der Daten steuern und die Daten an die Fähigkeiten der Geräte der Teilnehmenden anpassen. Es kann auch sein, dass die Durchführung von Mitschnitten einen Bestandteil des Angebots bildet. Daher ist es in der Regel unvermeidbar, dass zumindest bei dem Betreiberdienst auch befugte oder unbefugte Mitschnitte durchgeführt werden könnten, ob mit seinem Wissen oder gegen seinen Willen. Nur Dienste, bei denen die Daten auf dem einen Endgerät verschlüsselt werden und nur auf der Gegenstelle wieder entschlüsselt werden können – so genannte Ende-zu-Ende-Verschlüsselung – stellen sicher, dass keine derartigen Mitschnitte beim Betreiber erfolgen können.

Sie sollten wissen: Das Fernmeldegeheimnis schützt Sie bei der Nutzung von Videokonferenzsystemen nicht gegenüber dem Anbieter. Es erstreckt sich auf den Betreiber Ihres Internetanschlusses, nicht aber auf den Ihres

Videokonferenzdienstes. Dies ist eine Lücke im Gesetz, die der europäische Gesetzgeber erkannt hat. Er hat die Mitgliedsstaaten verpflichtet, bis zum Ende dieses Jahres den Schutz auf „interpersonelle Kommunikationsdienste“, darunter auf öffentliche Web- und Videokonferenzsysteme, auszuweiten. Diese werden dann die strengen Anforderungen des Telekommunikationsrechts zu erfüllen haben, einschließlich des Fernmeldegeheimnisses. Noch gelten aber die alten, lückenhaften Regeln.

Sie haben daher keine Wahl: Sie müssen dem Anbieter Ihres Videokonferenzdienstes vertrauen. Sie können ihn jedoch zumindest vertraglich binden. Dazu sind Sie auch verpflichtet. Denn damit tragen Sie nicht nur zum Schutz Ihrer eigenen Rechte bei, sondern auch zum Schutz Ihrer Beschäftigten und Kommunikationspartner/-innen. Was vertraglich zu regeln ist, gibt der Gesetzgeber vor. Seriöse Anbieter verfügen daher über einen Mustervertrag.

Allerdings wird Ihnen und den genannten Personen die Durchsetzung weit schwerer fallen, wenn Ihr Vertragspartner seinen Sitz außerhalb von Eueopäischer Union und Europäischem Wirtschaftsraum hat, sodass Sie sich im Konfliktfall an ein Gericht wenden müssten, das in einer fremden Rechtsordnung entscheidet, die Ihre Rechte womöglich nicht ebenso stark schützt wie die europäische. Um diesem Umstand entgegenzuwirken, hat die Europäische Kommission Standardvertragsklauseln entwickelt (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087). Nur deren vollständige Anwendung entfaltet jedoch den intendierten umfassenden Schutz Ihrer Interessen und der Interessen der betroffenen Personen. Die Pflichten aus den Standardvertragsklauseln dürfen daher nicht eingeschränkt werden.

Dieser Schutz erstreckt sich auch auf Risiken, die aus der Auswertung der Umstände der Kommunikation oder weiterer Daten für eigene Zwecke der Anbieter oder für Zwecke Dritter resultieren. Diese Risiken bestehen auch in der Bildung von Persönlichkeits- und Nutzungsprofilen der Gesprächsteilnehmer, die sich werblich, politisch oder auch durch Wettbewerber und zur Anwerbung von Personal missbrauchen lassen. Um eine solche Profilbildung auszuschließen, müssen Sie dem Anbieter eine derartige Auswertung untersagen. Viele Anbieter behalten sich die Auswertung jedoch in ihren Allgemeinen Geschäftsbedingungen vor. In einem solchen Fall wären individuelle Nutzungsvereinbarungen nötig. Erfolgversprechender erscheint ein Wechsel des Anbieters.

Empfehlungen

Als erstes sollten Sie prüfen, ob anstelle von Videokonferenzen auch Telefonkonferenzen ausreichen könnten, um die gewünschte Abstimmung untereinander herbeizuführen. Diese können sehr viel leichter datenschutzgerecht durchgeführt werden.

Sind Videokonferenzen nötig, ist es am besten, einen eigenen Dienst mit im Quelltext öffentlich verfügbarer Software (Open-Source-Software) bereitzustellen. Selbstverständlich ist auch der Einsatz kommerzieller Software möglich, solange gesichert ist, dass diese Software nicht ihrerseits Daten über Ihre Beschäftigten oder deren Kommunikationspartner/-innen an den Hersteller oder an Dritte für eigene Zwecke übermittelt. Sie können dabei auch auf die Unterstützung eines Dienstleisters für den Betrieb zurückgreifen. Leider ist es insbesondere für kleine Institutionen kaum mit verhältnismäßigem Aufwand leistbar, eine gut funktionierende datenschutzgerechte Lösung zu betreiben oder betreiben zu lassen.

Auf der nächsten Stufe empfehlen wir Ihnen zu prüfen, ob eine der Lösungen europäischer Anbieter Ihren Bedürfnissen entspricht. Erfüllt eine Lösung Ihre geschäftlichen Anforderungen, dann prüfen Sie, ob der Anbieter erwarten lässt, dass er die Daten nur im zulässigen Rahmen verarbeitet und insbesondere nicht entgegen europäischem Datenschutzrecht an Dritte – einschließlich ausländische Behörden – weitergibt, dass er ausreichende Datensicherheit (zum Beispiel durch Zertifizierung) nachweisen kann, Ihnen die Verschlüsselung der Datenübertragung garantiert und bereit ist, mit Ihnen einen gesetzeskonformen Auftragsverarbeitungsvertrag zu schließen.

Der Anbieter muss Ihnen gegenüber auch darlegen, ob er Dienstleister außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums zur Erbringung der Leistung hinzuzieht. Einige Anbieter fungieren lediglich als Wiederverkäufer von Leistungen US-amerikanischer Unternehmen. Andere lassen einen wesentlichen Teil der Dienstleistung von außereuropäischen Unternehmen der gleichen Unternehmensgruppe erbringen. In den beiden letztgenannten Fällen gewinnen Sie zwar einen europäischen vertraglichen Ansprechpartner. Jedoch ist auch dadurch nicht sichergestellt, dass der Anbieter sich im Konfliktfall an EU-Recht hält und nicht an sein lokales Recht.

Im letztgenannten Fall wie auch bei der direkten Beauftragung eines der außereuropäischen Anbieter mit signifikantem Marktanteil – in der Regel mit Sitz in den USA – müssen Sie neben den Fragen, die auch bei rein europäischen Anbietern eine Rolle spielen, die zusätzlichen Risiken bedenken und die rechtlichen Garantien prüfen.

Leider erfüllen auch einige der Anbieter, die technisch ausgereifte Lösungen bereitstellen, die datenschutzrechtlichen Anforderungen bisher nicht. Dies trifft derzeit (Stand 3. Juli 2020) z. B. auf die Dienste Blizz, Cisco WebEx, Cisco WebEx über Telekom, Google Meet, GoToMeeting, Microsoft Teams, Skype, Skype for Business Online und zoom zu. Mit NETWAYS Web Services Jitsi, sichere-videokonferenz.de, TixeoCloud, Werk21 BigBlueButton und Wire stehen allerdings Alternativen bereit, die die datenschutzrechtlichen Anforderungen erfüllen.

Für eine detaillierte Bewertung verweisen wir auf unsere „Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten“, die regelmäßig aktualisiert werden und die unter https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/corona-Pandemie.html verfügbar sind. Sollte der von Ihnen in Betracht gezogene Anbieter nicht in dieser Liste enthalten sein, finden Sie zur Erleichterung Ihrer Prüfung auf der genannten Webseite auch unsere „Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten“, die bestimmte häufig zu beobachtende Mängel in Auftragsverarbeitungsverträgen auflistet.

Organisatorische Regelungen

Vergessen Sie zum Schluss auch organisatorische Regelungen für die Videokonferenzen in Ihrer Institution nicht. Diese sollten das Vorgehen vorgeben, das einzuhalten ist, wenn eine Videokonferenz aufgenommen werden soll, und ggf. auch Bestimmungen enthalten, über welche Themen in einer Videokonferenz nicht gesprochen werden sollte. In den Regelungen sollten die Kontaktdaten von Personen aufgeführt werden, die in datenschutzrechtlichen Zweifelsfällen oder bei informationstechnischen Problemen Hilfestellung geben. Es sollte auch erläutert werden, wie vorzugehen ist, wenn eine Verletzung des Schutzes personenbezogener Daten vermutet wird.

Vor allem diejenigen Berufsgruppen, die mit besonders sensiblen Daten arbeiten, beispielsweise im medizinischen Kontext oder bei psychologischen Beratungen, sollten in besonderer Weise auf die Einhaltung datenschutzrechtlicher Grundsätze achten. Die Nutzung von Plattformen etwa zur videogestützten Online-Beratung beinhaltet oft eine Vielzahl von Risiken, die sorgsam mit den Vorteilen abgewogen werden müssen.

Fazit

Auch in dieser Zeit einer extrem beschleunigten und teilweise auch überstürzten Digitalisierung der Arbeitswelt muss der Schutz personenbezogener Daten immer mitgedacht werden. Dort, wo die Dringlichkeit der aktuell zu ergreifenden Maßnahmen dies nicht im notwendigen Umfang zulässt, muss kontinuierlich nachgebessert werden. Sollten datenschutzrechtliche Unwägbarkeiten oder gar Missstände auftreten, sind diese umgehend zu beheben.