Konsultation der Landesstelle der Psychologischen Beratungsstellen zur Online-Beratung mittels des Videokonferenzsystems Zoom bei der Aufsichtsbehörde

Verfasst am 12. Juli 2021

Bearbeitung bei der Außenstelle Süd des BfD-EKD: Dr. Axel Gutenkunst

Nach § 34 Abs. 9 DSG-EKD konsultiert eine verantwortliche Stelle, hier die Landesstelle der Psychologischen Beratungsstellen der Landeskirche Württemberg, vor einer Verarbeitung personenbezogener Daten die Aufsichtsbehörde, hier die Außenstelle Süd des Datenschutzbeauftragten der EKD, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechte der betroffenen Personen zur Folge hat oder haben kann.

Ergebnis der Konsultation:

Die Außenstelle sieht unter den folgenden Voraussetzungen den Schutz der personenbezogenen Daten der Ratsuchenden bei einer Beratungs-Videokonferenz mit dem Videokonferenzsystem Zoom (nachfolgend kürzer Beratungs-Videokonferenz) hinreichend sichergestellt:

1. Es wird die Ende-zu-Ende-Verschlüsselung des Videokonferenzsystems Zoom verwendet.
2. Die Verteilung der Links zu einer Beratungs-Videokonferenz erfolgt separat unter Verwendung eines E-Mail-Providers, der
    a. eine Ende-zu-Ende-Verschlüsselung betreibt und
    b. mittels eines Browsers genutzt werden kann.
3. Die Verwendung des Videokonferenzsystems Zoom erfolgt über einen Zwischenanbieter.
4. Ratsuchende werden vor ihrer erstmaligen Beratungs-Videokonferenz und dann bei Bedarf durch geeignete Maßnahmen (z.B. separate telefonische Beratung, zusenden eines Links eines anderen Videokonferenzanbieters) darin unterstützt, passende Endgeräte-Einstellungen zu finden, wenn sich technische Probleme zeigen.
5. Die Landesstelle macht Bildschirmkopien der Einstellungen, mit denen sie typischerweise Beratungs-Videokonferenzen einrichtet und startet und schickt sie an die Außenstelle Süd des BfD-EKD.
6. Beratungsstelle und Ratsuchende melden sich unter Verwendung von Pseudonymen bei der Beratungs-Videokonferenz an bzw. initialisieren diese.

Zu den Gründen:

Inhaltsverzeichnis

Rechtliche Aspekte

Rechtsgrundlage der Stellungnahme

Nach § 34 Abs. 5 DSG-EKD muss eine verantwortliche Stelle dann, wenn eine Form der Verarbeitung, insbesondere die Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zu hat, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchführen (Datenschutz-Folgenabschätzung). Was eine Datenschutz-Folgenabschätzung umfasst ist in § 34 Abs. 4 DSG-EKD ausgeführt.

Der Begriff „Risiko für die Rechte“ beinhaltet, dass nicht die betroffenen Personen darlegen müssen, wo sie Risiken hinsichtlich einer Beeinträchtigung ihrer persönlichen und sachlichen Verhältnisse sehen, sondern dass es vielmehr der verantwortlichen Stelle obliegt, Risiken zu erkennen und sie auf ein vertretbares Maß zu verringern.

Nach § 34 Abs. 9 DSG-EKD konsultiert die verantwortliche Stelle die Aufsichtsbehörde, wenn aus der Datenschutz-Folgenabschätzung einer geplanten Verarbeitung hervorgeht, dass diese ein hohes Risiko für die Rechte betroffener Personen zur Folge hat oder haben könnte.

Umfassender Verarbeitungsbegriff

Die Datenschutzgesetze, auch das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD), haben „*Verarbeitungen*“ von Daten im Blick. Dieser Begriff ist legal definiert (§ 4 Ziffer 3 DSG-EKD). Damit sind *Vorgänge* oder *Vorgangsreihen* gemeint. Bei diesen Vorgängen oder Vorgangsreihen kommen „*Verfahren*“ zum Einsatz. Solche *Verfahren* sind z.B. Programme, Datenbanken oder eben Videokonferenzsysteme. Es genügt für die Beurteilung der Datenschutzkonformität einer *Verarbeitung* deshalb nicht, lediglich ein *Verfahren* wie etwa ein bestimmtes Videokonferenzsystem in den Blick zu nehmen, sondern es muss der ganze Vorgang einer Beratungs-Videokonferenz unter Verwendung eines Videokonferenzsystems in den Blick genommen und auf Risiken hin beurteilt werden.
Dem wird durch die oben genannte Liste von Voraussetzungen Rechnung getragen.

Übermittlung personenbezogener Daten in das Drittland USA

Die Verwendung des Videokonferenzsystems Zoom der Firma ZOOM Video Communications, Inc (nachfolgend teilweise nur als Zoom bezeichnet) kann auch bei einer Ende-zu-Ende-Verschlüsselung (nachfolgend teilweise als E2EE bezeichnet) eine Übertragung von Daten in die USA mit sich bringen. Dass Videokonferenzen mit Zoom über einen in Deutschland stehenden Server laufen ändert rechtlich daran nichts, da nicht nur das aktive übertragen von Daten an Dritte, sondern auch das passive bereithalten für einen Zugriff Dritter auf Daten datenschutzrechtlich eine Offenlegung darstellt.

Die *neuen* Standardvertragsklauseln (SCC) der EU-Kommission vom 4.6.2021 sind Musterverträge, die ausreichende Garantien nach Art. 46 DSGVO für eine Datenübermittlung in Drittstaaten wie die USA darstellen können. Sie berücksichtigen die bisherige EuGH-Rechtsprechung (auch zum Privacy-Shield) und sind nunmehr sprachlich an die Bestimmungen der DSGVO angepasst. US-Anbieter, also auch Zoom, müssen in den nächsten 18 Monaten eine Aktualisierung auf die neuen SCC vornehmen.

Auch in den neuen SCC muss dargelegt werden, wie das vom EuGH beschriebene Risiko des Zugriffes auf Daten europäischer Bürger durch US-Behörden durch ergänzende Maßnahmen hinreichend verlässlich verringert wird. Das sind im wesentlichen weiterhin die Maßnahmen, die bereits bislang vom Europäischen Datenschutzausschuss EDSA (siehe https://de.wikipedia.org/wiki/Europ%C3%A4ischer_Datenschutzausschuss) vorgeschlagen wurden:

1. eine Verschlüsselung der Daten (hier eine „echte“ Ende-zu-Ende-Verschlüsselung)
2. eine effektive Pseudonymisierung
3. eine verteilte Verarbeitung in der Form, dass eine Partei allein nicht in der Lage ist, eine Identifizierung vorzunehmen.

Bezogen auf Beratungs-Videokonferenzen mittels des Videokonferenzsystems Zoom durch psychologische Beratungsstellen der Landeskirche Württemberg heißt das, dass geprüft werden muss, ob unter der Einhaltung der oben genannten Voraussetzungen, konkret realisiert durch

- das Videokonferenzsystem Zoom auf der Basis von E2EE
- den Zwischenanbieter Connect4Video (nachfolgend teilweise als C4V bezeichnet)
- den E-Mail-Provider ProtonMail (Ende-zu-Ende verschlüsselte E-Mails, Browsernutzung)

für die Ratsuchenden ein hinreichendes Datenschutzniveau gegeben ist.

Zusätzliche rechtliche Voraussetzungen für kirchliche Stellen

Eine kirchliche Stelle, die Zoom mittels des Auftragsverarbeiters C4V einsetzen will, muss mit C4V einen Vertrag über eine Datenverarbeitung im Auftrag nach § 30 DSG-EKD abzuschließen.
Nach § 30 Abs. 3 Satz 1 DSG-EKD müssen Auftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen ausgewählt werden. Dies bedeutet, dass

a) die Firma Connect4Video ihrerseits auf der Basis der Standardvertragsklauseln der EU vertraglich einen hinreichenden Schutz der personenbezogenen oder personenbeziehbaren Daten ihrer Auftragsgeber, die unvermeidlich an die US-Firma Zoom übermittelt werden bzw. auf die die US-Firma Zoom zugreifen könnte, bewirkt und
b) ihren Kunden „Landesstelle der Psychologischen Beratungsstellen“ dahingehend unterstützt oder es diesem ermöglicht, dass bei dessen Beratungs-Videokonferenzen an die US-Firma weitestgehend nur pseudonymisierte Zugangsdaten übermittelt werden (z.B. Verwendung von „Landesstelle“ als Benutzername anstatt „Landesstelle der psychologischen Beratungsstellen der Landeskirche Württemberg“ oder Anmeldung über eine separate bei ProtonMail eingerichtete E-Mail-Adresse zur Verteilung der Links)

um den vom Europäischen Datenschutzausschuss EDSA (siehe https://de.wikipedia.org/wiki/Europ%C3%A4ischer_Datenschutzausschuss) vorgeschlagen Maßnahmen

1. effektive Pseudonymisierung
2. verteilte Verarbeitung in der Form, dass eine Partei allein nicht in der Lage ist, eine Identifizierung vorzunehmen.

Rechnung zu tragen.
Ferner muss C4V einen Vertrag über eine Datenverarbeitung im Auftrag (AVV) der Bezug auf die DSGVO nimmt, die für solche Fälle vom Beauftragten für den Datenschutz in der Evangelischen Kirche in Deutschland (BfD-EKD) entwickelten Zusatzvereinbarung unterzeichnen (siehe https://datenschutz.ekd.de/infothek-items/av-vertrag/). Dem ist beim genannten Anbieter C4V so.

Fazit der rechtlichen Voraussetzungen

Die (an sich unproblematischen) vertraglichen Voraussetzungen (AVV zwischen der Landesstelle und C4V, AVV zwischen C4V und Zoom, SCC zwischen C4V und Zoom) einer Beratungs-Videokonferenz mittels des Videokonferenzsystems Zoom sind gegeben.
Aber selbst SCC mit Ergänzungen zwischen dem Auftragnehmer C4V und Zoom würden der Anforderung des EuGH, Zugriffe der US-Geheimdienste auf Beratungsdaten zu unterbinden, nicht genügen.
Dieser Anforderung wird aber durch die ergänzend getroffenen *Maßnahmen* (E2EE, Pseudonymisierung, Zwischenanbieter, separate Verteilung der Links über einen europäischen Mail-Provider) hinreichend Rechnung getragen.

Technische Aspekte

Technische Anforderungen an die Endgeräte

Es ist nicht zu erwarten, dass eine Videokonferenz auf E2EE-Basis bei Verwendung des Videokonferenzsystems Zoom erhöhte Anforderungen an die Endgeräte des Gastgebers und der Teilnehmer (z.B. PCs oder Notebooks) stellt, da dieses Videokonferenzsystem schon bisher die Daten verschlüsselt zu und von den Endgeräten übertragen hat[1].
Allerdings wurden bislang die Schlüssel serverseitig erzeugt und an die Teilnehmer verteilt. Bei einer Zoom-Videokonferenz mit E2EE erzeugen Gastgeber und Teilnehmer lokal auf ihren Endgeräten private und öffentliche Schlüssel[2] („echte“ E2EE-Verschlüsselung) und verteilen damit einen *vom Gastgeber* generierten Sitzungsschlüssel. Der verwendete Server der US-Firma Zoom wird damit zu einem „blinden“ Verteiler der Datenpakete mit den Audio- und Videosignalen.
Die mit der Schlüsselverwaltung verbundene Last ist gering und die Verteilung der Schlüssel erfolgt vor der eigentlichen Videokonferenz.

Nutzung einer echten E2EE zwischen zwei Teilnehmern

Schon bislang gab es wohl die Möglichkeit einer „echten“ verschlüsselten Kommunikation zwischen zwei Teilnehmern (möglicherweise auf der Basis eines Schlüsselaustauschs mittels Diffie-Hellmann[3]).
Diese Verschlüsselungsmöglichkeit wird nicht weiter untersucht, da das hinter einer echten E2EE stehende Verfahren beim Videokonferenzsystem Zoom auch mit nur zwei Teilnehmern verwendet werden kann.

Verteilung der Einladungslinks mittels E2E-E-Mail-Provider

Die Schweigepflicht nach § 203 StGB umfasst nicht nur Beratungsinhalte, sondern bereits den Umstand, eine Beratungsstelle aufzusuchen oder aufgesucht zu haben.
Dieser Anforderung wird dadurch entsprochen, indem die Verteilung der Links für eine Teilnahme an einer Beratungs-Videokonferenz nicht mittels des Anbieters C4V oder mittels der US-Firma Zoom, sondern mittels eines separaten (europäischen) E-Mail-Providers erfolgt, der die Teilnahmelinks Ende-zu-Ende-verschlüsselt zustellt (ProtonMail, siehe

---

[1] GCM-Verschlüsselung, siehe https://de.wikipedia.org/wiki/Galois/Counter_Mode

[2] https://de.wikipedia.org/wiki/Schl%C3%BCssel_(Kryptologie)#Schl%C3%BCssel_bei_asymmetrischen_Verfahren

[3] https://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch

https://de.wikipedia.org/wiki/ProtonMail). Damit bekommt insbesondere die US-Firma Zoom die E-Mail-Adressen der Konferenzteilnehmer nicht mit (siehe EuGH-Urteil).
Ferner wird es den Ratsuchenden ermöglicht, eine Beratungs-Videokonferenz aus ihrem familiären Umfeld oder aus ihrem Haushalt heraus so in Anspruch zu nehmen, dass sie selbst bestimmen können, wem dies bekannt wird und wem nicht. So könnten sie sich selbst ein (kostenfreies) ProtonMail-Konto einrichten und dieses mit ihrem Browser betreiben. Ihr bisheriges E-Mail-Konto, auf das möglicherweise weitere Personen Zugriff haben oder nehmen könnten, würde davon nichts mitbekommen.

Probeläufe

Auch versierte Teilnehmer an Videokonferenzen stellen immer wieder fest, dass „irgendwas“ (Lautsprecher, Mikrofon, Kamera, Internetverbindung) nicht so funktioniert wie es für die Videokonferenz erforderlich ist. Bei häufigen Videokonferenzen zeigt sich dann im Laufe der Zeit, wo die Ursachen liegen und wie Abhilfe geschaffen werden kann.
Auch wenn anzunehmen ist, dass nur Personen, die Kenntnisse im Umgang mit Notebooks oder Computern haben, die Möglichkeit einer Beratungs-Videokonferenz aufgreifen, muss die Beratungsstelle dafür Sorge tragen, dass solche technischen Probleme keine ungewollten Offenbarungen nach sich ziehen (die eingangs genannte Voraussetzung Ziffer 4).
Dazu teilt die Beratungsstelle den Ratsuchenden zum Mindesten eine Telefonnummer mit, unter der diese bei Unsicherheiten oder technischen Problemen bei der Beraterin oder dem Berater nachfragen können. Falls dies nicht ausreicht, könnte unter Nutzung eines europäischen Anbieters, bei dem verlässlich davon ausgegangen werden kann, dass es nicht zu unrechtmäßigen Datenspeicherungen kommt, ein Testlauf angeboten werden[4].

Anmerkung zu zertifizierten Videokonferenzsystemen

Es gibt zertifizierte Videokonferenzsysteme, die von Beratungsstellen verwendet werden könnten.
Es ist allgemein anerkannt, dass bei einer „echten“ Verschlüsselung, d.h. wenn die Schlüssel ausschließlich beim Sender und Empfänger liegen, Daten in hohem Maße vor einer unbefugten Kenntnisnahme geschützt sind.
Es ist davon auszugehen, dass auf der Basis einer echten E2EE ein gleichwertiger wenn nicht höherer Schutz vor einer unbefugten Kenntnisnahme realisiert wird wie durch die Verwendung eines Videokonferenzsystems, bei dem zwar umfangreiche technische und organisatorische Maßnahmen getroffen werden, aber die Videokonferenzdaten auf dem verwendeten Server unverschlüsselt vorliegen bzw. die Schlüssel dem Serverbetreiber bekannt sind (weil lediglich der Transport der Daten zum und vom Server verschlüsselt erfolgt).
Da die Schweigepflicht nach § 203 StGB für Beraterinnen und Berater persönlich gilt, müssen auch bei einer Beratungs-Videokonferenz entsprechende organisatorische und technische Maßnahmen getroffen werden. Mittlerweile werden rechtlich auch IT-Dienstleister in den Kreis der Schweigepflichtigen nach § 203 StGB einbezogen, so dass rechtlich auch dann ein Schutz vor einer unbefugten Offenbarung gegeben ist, wenn die Nutzung von IT-Ressourcen die Möglichkeit beinhalten, dass Mitarbeitenden des entsprechenden Dienstleisters vertrauliche Inhalte zu Kenntnis nehmen könnten.
Die Vertraulichkeit von Beratungsinhalten bleibt jedoch verlässlicher gewahrt, wenn IT-Dienstleister erst gar nicht die Möglichkeit einer Kenntnisnahme haben, weil die Daten, auf die sie zugreifen könnten, verschlüsselt sind.
Dass im Bereich von Beratungs-Videokonferenzen überhaupt Videokonferenzsysteme ohne echte E2EE eingesetzt werden ist datenschutzrechtlich insoweit noch vertretbar, als die Möglichkeit einer E2EE bislang nicht oder nur mit einem kaum leistbaren Aufwand technischer und/oder finanzieller Art bestand und damit, zum Nachteil von Ratsuchenden, überhaupt keine Beratungs-Videokonferenzen hätten angeboten werden können. Künftig dürfte eine echte E2EE jedoch verpflichtender Standard werden.

[4] z.B. https://www.eckd-kigst.de/news/news-lesen/news/itmmeet-nutzen-sie-eine-kostenfreie-einfache-und-sichere-videokonferenzloesung

Das Optimum wären Beratungs-Videokonferenzen auf der Basis einer echten E2EE unter Verwendung eines europäischen Anbieters des Videokonferenzsystems.
Die eigentliche datenschutzrechtliche Frage ist dann, ob die Nutzung eines europäischen Anbieters eines Videokonferenzsystems nach den geltenden Datenschutzbestimmungen als unabdingbar zu beurteilen ist oder ob es die DSGVO und das DSG-EKD zulassen, dass unter den eingangs genannten Voraussetzungen auch eine US-Firma als Anbieter eines Videokonferenzsystems einbezogen werden kann. Letzteres wird im Rahmen dieser Konsultation seitens der Außenstelle Süd beim BfD-EKD bejaht.

Fazit der technischen Aspekte

Die hinter einer Beratungs-Videokonferenz stehenden technischen Komponenten sind komplex. Die Links zur Teilnahme an einer Beratungs-Videokonferenz werden mit einem E-Mail-System

Schutz der Ratsuchenden

Verteilung des Links zur Teilnahme an einer Beratungs-Videokonferenz

Die Links zur Teilnahme an einer Beratungs-Videokonferenz werden mit einem E-Mail-System mit einer Ende-zu-Ende-Verschlüsselung verschickt (ProtonMail, siehe https://de.wikipedia.org/wiki/ProtonMail) und nicht mittels Optionen des Zoom-Videokonferenzsystems und auch nicht mittels des Auftragnehmers Connect4Video.
Der Schutz der Ratsuchenden wird dabei wie folgt bewirkt:

a) Sie können, da ProtonMail in ihrem Web-Browser läuft, die E-Mail-Korrespondenz im Zusammenhang mit ihrer Beratungs-Videokonferenz neben ihrem sonst verwendeten Postfach und neben dem sonst verwendeten E-Mail-Client abwickeln, beispielsweise wenn das von ihnen verwendete Endgerät von weiteren Personen genutzt wird.
b) Die Beratungsstelle kann den Ratsuchenden auch E-Mails an ihre sonst verwendete E-Mail-Adresse schicken, wenn diese kein kostenloses Postfach bei ProtonMail einrichten wollen, diese aber mit einem zuvor telefonisch vereinbarten Kennwort schützen.
c) Die Ende-zu-Ende-verschlüsselte E-Mail kann auf dem Übertragungsweg nicht eingesehen werden.

Da für eine Beratungsstelle nur bedingt absehbar ist, wer sonst noch im Haushalt oder im Umfeld der ratsuchenden Person auf welche Weise auf das von dieser verwendete Endgerät Zugriff nehmen kann, muss sie eine Vorgehensweise anbieten können, die es den Ratsuchenden einigermaßen verlässlich erlaubt, selbst zu bestimmen, wer über ihre Inanspruchnahme einer Beratungs-Videokonferenz informiert ist.

Da solche Produkte wie ProtonMail nicht allgemein bekannt sind, muss die Beratungsstelle auch diesbezüglich für die Ratsuchenden verständliche Nutzungs-Informationen bereithalten (die eingangs genannte Voraussetzung Ziffer 4).

Identifikation mittels IP-Adresse

Die US-Firma Zoom bekommt zwangsläufig die IP-Adresse der Beratungsstelle und die IP-Adresse der ratsuchenden Person mit, sonst könnten die Datenpakete mit den Audio- und Videoinformationen nicht übertragen werden.

Eine IP-Adresse identifiziert allerdings nicht eine bestimmte Person, sondern den Router, über den der Zugang zum Internet hergestellt wird. Hinter diesem Router kann eine ganze Familie oder ein ganzer Haushalt mit einer ganzen Palette von Endgeräten stehen. Auch dieser Personenverbund ist nicht eindeutig bestimmt, z.B. wenn Gäste (Freunde, Bekannte) zu Besuch sind. Hinter einer IP-Adresse kann auch eine Firma mit einer Vielzahl von Mitarbeitenden stehen. Eine konkrete Identifikation des Endgeräts, mit dem zu einem bestimmten Zeitpunkt eine Videokonferenz durchgeführt wird, wäre nur anhand der Protokolle des verwendeten Routers möglich. Selbst dann würde nur das Endgerät identifiziert, aber nicht die Person, die das Endgerät verwendete. Allerdings bewirkt die

zunehmende Verwendung der längeren IPv6-Adressen, dass auch Routern von Privatpersonen eine feste IPv6-Internetadresse auf Dauer zugeordnet wird und nicht, wie aufgrund des beschränkten Adressraums von IPv4 bislang, immer wieder wechselnd.

Einem Versuch seitens der US-Firma Zoom, anhand der IP-Adresse auf die dahinterstehende Person oder Stelle zu schließen, würde entgegenstehen, dass europäische Internet-Provider nur auf der Basis einer richterlichen Anordnung offenlegen würden, welcher Person oder Stelle eine bestimmte IP-Adresse für welchen Zeitraum zugewiesen wurde.

Das technische Datum IP-Adresse zur Identifikation von Personen zu nutzen wäre zum einen ein Verstoß gegen die DSGVO. Zum anderen ist schwer vorstellbar, dass die US-Firma Zoom seitens der US-Justiz aufgefordert würde, technische Möglichkeiten zu nutzen, um ggf. unter Verstoß gegen EU-Recht im Zusammenhang mit Videokonferenzen verwendete IP-Adressen bestimmten Personen oder Stellen zuzuordnen. Rechtlich würde dies über das zur Verfügung stellen gespeicherter Geschäftsdaten im Rahmen von Ermittlungsverfahren hinausgehen und wäre eher als Aufforderung zur geheimdienstlichen Tätigkeit anzusehen.

Dafür, dass das EuGH-Urteil so weit auszulegen ist, dass auch dies verhindert werden muss bzw. dass auch in Rechnung gestellt werden muss, dass die US-Justiz zu solchen Maßnahmen auffordern könnte, gibt es keine Anhaltspunkte.

Unabhängig davon muss eine Beratungsstelle zum Schutz der Ratsuchenden bei der Verwendung von Zoom dafür Sorge tragen, dass bei einer Videokonferenz möglichst keine sie identifizierenden Angaben gemacht werden. Eben dazu wird der Zwischenanbieter Connect4Video und ein von diesem bereitgestellten Kunden-Account genutzt. Die Beratungsstelle selbst ist kein Kunde der US-Firma Zoom.

Eine Besonderheit stellt es dar, wenn eine ratsuchende Person, die sich bei Zoom registriert hat, weil sie Zoom auch für andere Zwecke nutzt, an einer Beratungs-Videokonferenz teilnimmt. Eine solche Person hätte die Option, die Beratung an einem anderen Ort (Freunde, Bekannte, Arbeitsstelle, Internet-Café, ...) durchzuführen, um sich der Möglichkeit einer Identifikation durch die Firma Zoom anhand ihrer IP-Adresse zu entziehen. Eine weitere Option wäre, für die Dauer der Beratung eine VPN-Verbindung, etwa angeboten durch die Mozilla-Foundation, zu nutzen.

Aus dem Interesse heraus, als vertrauenswürdiger Geschäftspartner angesehen zu werden, dürfte die US-Firma Zoom generell davon Abstand nehmen, mittels der IP-Adressen unzulässige Identifikationen zu bewerkstelligen. Auch insofern bleibt im Ergebnis festzustellen, dass das Risiko einer Identifikation der Beratungsstelle oder der ratsuchenden Person anhand der IP-Adresse im Zusammenhang mit einer Beratungs-Videokonferenz unter den genannten Voraussetzungen hinreichend gering ist,

Identifikation anhand sog. Browser-Fingerprints

Es ist davon auszugehen, dass die für die Videokonferenz verwendeten Browser auf den Endgeräten der Teilnehmer die übliche Fülle an technischen Information an den Zoom-Server übermitteln. Aus dieser Fülle an Informationen lassen sich sog. Browser-Fingerprints errechnen, die geeignet sein könnten, die Teilnehmer an einer Beratungs-Videokonferenz zu identifizieren.

Datenschutzrechtlich wäre es zulässig, dass die US-Firma Zoom die von den Browsern übermittelten technischen Daten dazu verwendet, die korrekte oder optimale Darstellung der Videokonferenz in den Browsern der Teilnehmer zu bewirken. Für eine darüberhinausgehende Speicherung dieser Daten als Browser-Fingerprint müsste die US-Firma die Einwilligung der Teilnehmenden einholen, sonst läge ein Verstoß gegen die DSGVO vor.

Anhand des Browser-Fingerprints könnte seitens der US-Firma Zoom mit einer unter Umständen hohen Wahrscheinlichkeit ein für eine Videokonferenz verwendeter Browser wiedererkannt werden. Würden dann mit demselben Browser auf der Homepage der US-

Firma Zoom identifizierende Angaben gemacht, etwa im Zuge einer Registrierung, könnte der Browser-Fingerabdruck der betreffenden Person oder Stelle zugeordnet werden.

Auch aus diesem Grunde muss es eine Beratungsstelle vermeiden, direkt mit der Firma Zoom über deren Homepage in Kontakt zu treten, etwa um eine Lizenz zu erwerben, sondern der eingangs gemachten Voraussetzung entsprechen und die Zugangsdaten vermittelt durch einen Zwischenanbieter wie etwa Connect4Video erwerben.

Falls ratsuchende Personen selbst einen Benutzer-Account bei Zoom erworben haben, könnten sie seitens der Firma Zoom anhand des Browser-Fingerabdrucks (unter Begehung eines Rechtsverstoßes, s.o.) identifiziert werden. Sie könnten sich dem eventuell dadurch entziehen, indem sie für die Beratungs-Videokonferenz einen anderen Browser verwenden. Die Installation eines weiteren Browsers, wenn nicht bereits vorhanden, könnte dasselbe bewirken. Da aber der nunmehr andere Browser-Fingerabdruck serverseitig zur selben IP-Adresse gehört, dürfte die Schutzwirkung dieser Maßnahme begrenzt sein, würde es die US-Firma Zoom wirklich darauf anlegen, Videokonferenzteilnehmer anhand ihrer technischen Daten zu identifizieren. So könnte sie Skripte oder Programme einsetzen, die z.B. darauf ausgerichtet sind, zu erkennen, dass geänderte Browser-Fingerprints zur selben IP-Adresse gehören. Eine reelle Chance, sich solchen Ausspähungen zu entziehen, hätten Ratsuchende kaum. Selbst wenn sie auf der Basis einer Virtualisierung ein anderes Betriebssystem verwenden würden, wären zwar die Browser-Fingerprints verschieden, könnten aber über die gleiche IP-Adresse einander zugeordnet werden, auch dann noch, wenn ein anderes Endgerät verwendet würde.

Allerdings würde sich die US-Firma Zoom beim Einsatz solcher Möglichkeiten in die Abhängigkeit der Beschäftigten begeben, die davon wissen. Mutmaßlich hat die US-Firma Zoom das größte Interesse daran, nachweisen zu können, dass ihre serverseitigen Programme „sauber“ sind.

Letztlich müssen Ratsuchende aber darauf vertrauen, dass die US-Firma Zoom vorhandene Möglichkeiten, sie anhand technischer Daten indirekt zu identifizieren ungenutzt lässt und dass die Zusage, die DSGVO einzuhalten, der Wahrheit entspricht. Dafür, dass dem so ist, spricht, dass die US-Firma Zoom existentiell darauf angewiesen ist, dass ihr Kunden, dazu gehören auch namhafte Firmen, vertrauen.

Insofern bleibt auch hier im Ergebnis festzustellen, dass das Risiko einer Identifikation der Beratungsstelle oder der ratsuchenden Person anhand der technischen Daten (Browser-Fingerprints) im Zusammenhang mit einer Beratungs-Videokonferenz mittels Zoom unter den genannten Voraussetzungen hinreichend gering ist.

Identifikation mittels des Zoom Clients

Es wäre denkbar, dass der Zoom-Client, den die Ratsuchenden bei einer E2EE-Konferenz herunterladen und installieren müssen, nicht nur die Übertragung der Audio- und Videodaten bewerkstelligt, sondern der dauerhaften Identifikation der Endgeräte dient (z.B. bereits anhand der langen Versionsnummer). Es würde dann dieselbe Sachlage wie bei den IP-Adressen und den Fingerprints eintreten, d.h. der US-Firma Zoom stünde eine weitere Option zur Verfügung, Teilnehmer an Videokonferenzen zu identifizieren.
Allerdings gibt es hinreichend viele Personen, die technisch in der Lage sind, Datenströme ihrer Endgeräte zu analysieren und dies auch tun. Ein Zoom-Client, der über seinen eigentlichen Zweck hinausgeht und Teilnehmer an Videokonferenzen ausspäht, wäre wohl längst als solcher erkannt und publik gemacht worden. Würde so etwas bekannt, hätte dies solche geschäftsschädigenden Folgen für die US-Firma Zoom, dass davon ausgegangen werden kann, dass diese selbst das allergrößte Interesse daran hat, dass ihr Client seriös agiert.

Fazit der Überlegungen zum Schutz der Ratsuchenden

Es sind auf der technischen Ebene eine Fülle von Möglichkeiten denkbar, wie die US-Firma Zoom, aber auch die anderen an einer Beratungs-Videokonferenz beteiligte IT-Dienstleister schon die dabei anfallenden technischen Daten dazu verwenden könnten, die an einer

Beratungs-Videokonferenz teilnehmenden Ratsuchenden zu identifizieren (die vorstehend angesprochenen Möglichkeiten sind nur die offensichtlichsten).

Dies Aussage, dass die eingangs genannten Voraussetzungen dies immer erfolgreich vereiteln, kann nicht gemacht werden. Diese Absolutheit wird aber weder von der DSGVO noch vom DSG-EKD noch vom EuGH gefordert.

Auch bei einer „Offline“-Beratung in angemieteten Räumlichkeiten in einem Innenstadtbereich kann es dazu kommen, dass der Umstand einer Inanspruchnahme einer psychologischen Beratung ungewollt weiteren Personen bekannt wird.

Schließlich muss auch bedacht werden, dass Ratsuchende eine Beratungs-Videokonferenz nicht zum Spaß machen, sondern weil sie sich in einer Notlage sehen.

Mit Blick auf diese Sachverhalte ergibt sich die Einschätzung, dass unter den eingangs genannten Voraussetzungen der Schutz der personenbezogenen Daten der Ratsuchenden auch bei einer Beratungs-Videokonferenz g mit dem Videokonferenzsystem der US-Firma Zoom hinreichend sichergestellt ist.