COMPLIANCE-ANFORDERUNGEN AN DEN EINSATZ VON VIDEOKONFERENZ-DIENSTEN

Isabell Conrad

Bevor die Corona-Pandemie Deutschland erreicht hatte, schien hierzulande undenkbar, dass nahezu alle Arbeitgeber und Dienstherren – auch Wirtschaftskanzleien, Banken bis hin zum Staat – innerhalb weniger Wochen flächendeckend Homeoffice und Videokonferenzen einführen. Selbst universitäre Prüfungen sollen teilweise mittels Webcam abgehalten werden. Noch 2016 hatte sich die Berliner Datenschutzbehörde sehr restriktiv geäußert, als das Bezirksamt Berlin Bewerbungsgespräche mit Bewerbern, die aus dem Ausland hätten anreisen müssen, per Skype durchführen wollte.[1] In Zeiten von Kontaktbeschränkungen geht es nicht mehr um das Ob, sondern nur noch um das Wie und der Trend lässt sich nicht mehr zurückdrehen.

Die Webconferencing-Anbieter gehören zu den Unternehmen, denen die Corona-Pandemie erhebliche Zuwächse beschert hat.[2] Gleichzeitig warnen Datenschützer vor nicht unerheblichen Datenabflüssen zu Drittdiensten und Verwendung der Daten zu eigenen Zwecken der Tool-Anbieter.[3] „Ein wesentliches Risiko besteht darin, dass bei der Videokonferenz unbefugt mitgehört oder sie aufgezeichnet und die Inhalte weiter ausgewertet werden, möglicherweise zum Nachteil der Personen, die an der Konferenz teilgenommen haben oder über die gesprochen wurde“, warnt die Berliner Datenschutzbehörde.[4] Microsoft hat am 6.5.2020 öffentlich Stellung genommen und kommt zum Ergebnis, dass die von der Berliner Datenschutzbehörde aufgezeigten Risiken im Hinblick auf die Nutzung von Microsoft Teams und Skype for Business Online nicht bestehen sollen.[5]

Prominente Fälle zeigen, dass teilweise die per Default standardmäßig eingestellten Sicherheitsmaßnahmen nicht ausreichen oder von den Nutzern unzureichend angewendet werden. So hat z. B. das bayerische Innenministerium die Videokonferenz-Software Cisco Jabber unter der Domain video.bayern.de betrieben. Die URLs der virtuellen Konferenzräume waren nach dem Schema video.bayern.de/Pfad/Raumnummer aufgebaut, wobei der „Pfad“ aus wenigen Buchstaben und die „Raumnummer“ aus sechs Ziffern bestand. Das Magazin c’t hat sich dieses Schema erschlossen und konnte an einer internen Sitzung des Innenministers zum Coronavirus „als Gast“ teilnehmen, ohne dass ein PIN erforderlich war.[6]

Im medizinischen Bereich wird schon seit Längerem die „Videosprechstunde“, also die telemedizinisch gestützte Betreuung von Patienten, gefördert.[7] Zumindest Kassenärzte dürfen nur zertifizierte Videokonferenzanbieter einsetzen und die Kassenärztliche Bundevereinigung hat eine Liste der zertifizierten Anbieter veröffentlicht.[8] Die Arztpraxen, die die Videosprechstunde einsetzen wollen, müssen dies der zuständigen Kassenärztlichen Vereinigung anzeigen und sich genehmigen lassen.[9]

Ein vergleichbar standardisiertes Vorgehen gibt es für Anwaltskanzleien derzeit nicht. Die Berliner Datenschutzbehörde empfiehlt: „Berufsgeheimnisträger dürfen nur Dienstleister einsetzen, die bei einem Vertraulichkeitsbruch strafrechtlich belangt werden können.“[10] Das Betreiben eines Videokonferenz-Dienstes hat zwar viele Aspekte eines Kommunikationsdienstes, aber die Einordnung als Fernmeldegeheimnis-verpflichteter TK-Dienst ist strittig. Der EuGH[11] und das OVG Münster[12] haben die Einordnung von Googles Mail-Dienst Gmail als TK-Dienst verneint. Zuvor hatte der EuGH hinsichtlich der VoIP-Funktion SkypeOut das Vorliegen eines elektronischen Kommunikationsdienstes im Sinne der Richtlinie 2002/21/EG bejaht.[13] Der umstrittene Entwurf der E-Privacy-Verordnung, der zeitgleich mit der DSGVO in Kraft treten, die Richtlinie 2002/58/EG ersetzen und die Anwendung der strengen Vertraulichkeitsregeln auf sog. „interpersonelle Kommunikationsdienste“ klarstellen sollte, ist vorerst gescheitert. Ein neuer Entwurf ist noch nicht in Sicht und mit einem Inkrafttreten frühestens 2024 zu rechnen.

1 Bln BDI, Jahresbericht 2016, S. 116, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2016-Web.pdf
2 Beispielsweise ist der Börsenwert des US-Anbieters ZOOM im März 2020 in die Höhe geschossen: Handelsblatt-Meldung v. 30.3.2020, https://www.handelsblatt.com/technik/it-internet/it-branche-neue-datenschutz-vorwuerfe-gegen-videodienst-zoom/25700760.html?ticket=ST-808899-uloKBgKawQuWNzbv5smE-ap6
3 https://www.heise.de/newsticker/meldung/New-Yorker-Staatsanwaeltin-prueft-Datenschutz-bei-Konferenz-App-Zoom-4694352.html; https://www.zeit.de/digital/datenschutz/2020-04/videodienst-zoom-datenschutz-hacker-angriffe-videokonferenzen
4 Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, v. 30.3.2020
5 https://news.microsoft.com/de-de/stellungnahme-zum-vermerk-berliner-datenschutzbeauftragte-zur-durchfuehrung-von-videokonferenzen-waehrend-der-kontaktbeschraenkungen/
6 https://www.heise.de/ct/artikel/c-t-deckt-auf-Bayerischer-Innenminister-bespricht-Corona-Krise-in-ungeschuetzter-Videokonferenz-4680288.html
7 https://www.kbv.de/html/videosprechstunde.php
8 https://www.kbv.de/media/sp/Liste_zertifizierte_Videodienstanbieter.pdf
9 https://www.kbv.de/media/sp/PraxisInfo_Coronavirus_Videosprechstunde.pdf
10 Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, v. 30.3.2020, S. 2.
11 EuGH Urteil v. 13.6.2019, C-193/18
12 OVG Münster, Beschl. v. 5.2.2020 – 13 B 1494/19
13 EuGH Urteil v. 5.6.2019, C-142/18

Videokonferenzsysteme sind häufig so angelegt, dass beim Betreiber die unverschlüsselten Bilder und Töne zusammenlaufen. Bei vielen Diensten kann nicht z. B. durch Verschlüsselung ausgeschlossen werden, dass der externe Videokonferenz-Anbieter Audio- und Videodaten und in der Konferenz geteilte Dokumente zur Kenntnis nehmen kann. Wenn innerhalb einer Videokonferenz vertrauliche Inhalte besprochen oder sensible Daten ausgetauscht werden (was z. B. bei einem Gespräch zwischen Mandant und Anwalt regelmäßig der Fall ist), sollen – so die gängige Empfehlung[14] – möglichst nur Anbieter innerhalb der EU oder EFTA eingesetzt werden. Allerdings müsste dann weiter geklärt werden, ob die europäischen Anbieter ihrerseits (als Subunternehmer) Cloud-Betreiber aus Drittstaaten einsetzen und ob diesen gegenüber die Kenntnisnahme-Möglichkeit hinsichtlich Inhalten der Videokonferenz oder Nutzungsdaten durch Verschlüsselung und entsprechender Schlüsselverwaltung ausgeschlossen ist.

Der folgende checklistenartige Leitfaden fasst – ohne Bezug zu konkreten Videokonferenz-Diensten oder -Produkten – gängige Empfehlungen zusammen, um Datenschutz-, IT-Sicherheits- und Urheberrechtsanforderungen einzuhalten.

1. **Keine Verbraucher-Version für Kanzlei-Zwecke:** Der Einsatz von (ggf. kostenlosen) Versionen, die vom Videokonferenz-Anbieter nur für Verbraucher (privaten Einsatz) bestimmt sind, ist für die dienstliche Nutzung durch Anwälte ausgeschlossen. Anderenfalls drohen Lizenzverstöße, was auch urheberrechtlich strafbar sein und zu erheblichen Schadensersatzforderungen des Anbieters (Stichwort: entgangene Lizenzgebühren) führen kann. Das gilt grundsätzlich auch für testweise Nutzung. Viele Tool-Anbieter erlauben Business-Kunden (wozu Anwaltskanzleien gehören) eine kostenlose Testphase.

2. **Datenflüsse und Transparenz der Leistungskette:** Das betrifft Inhaltsdaten (Content), Nutzungsdaten bzw. Telemetriedaten (u. a. Logfiles und IP-Adressen) sowie Stammdaten der Anwaltskanzlei als Kunde des Dienstanbieters. Erst nach Offenlegung kann die datenschutzrechtliche Rechtmäßigkeit beurteilt werden. Diese Beurteilung ist Voraussetzung für die Beauftragung. Gesondert offengelegt werden muss, wenn Daten in Länder außerhalb EU/EWR transferiert werden oder wenn von solchen Ländern aus (etwa im Rahmen von Support-Hotlines des Tool-Anbieters) auf personenbezogene Daten, die dem EU-Recht unterliegen, zugegriffen werden kann. Für solche Datenübermittlungen in Drittländer sind ggf. besondere vertragliche Regelungen mit dem Dienstanbieter erforderlich (z. B. sog. EU-Standarddatenschutzklauseln). Erste Informationen bietet die Datenschutzerklärung des Anbieters.

3. **Einsatz von Auftragsverarbeitern:** Im Regelfall ist erforderlich, dass der Anbieter sicherstellt, Inhaltsdaten (Content), Nutzungsdaten bzw. Telemetriedaten (u. a. Logfiles und IP-Adressen) nur zur Durchführung des Auftrags und nur für den Kunden und auf Weisung des Kunden zu verarbeiten. Datenschutzrechtlich dürften dem Dienstanbieter im Regelfall nur auf Basis eines sog. Auftragsverarbeitungsvertrags personenbezogene Daten zugänglich gemacht werden.[15] Will der Anbieter die vorgenannten Daten z. B. auch für die Weiterentwicklung seiner Dienste verwenden oder zu anderen Zwecken auswerten, liegt insoweit ggf. keine Verarbeitung „im Auftrag der Anwaltskanzlei" vor, sondern eine Verarbeitung zu eigenen Geschäftszwecken des Anbieters. Das ist im Regelfall bei personenbezogenen Daten nicht erlaubt, kann aber ggf. zulässig sein, soweit der Anbieter die Daten vorher anonymisiert. Daher ist vor der Auswahlentscheidung der Anwaltskanzlei eine hinreichend konkrete und detaillierte Offenlegung durch den Toolanbieter wichtig, ob und inwieweit er ggf. Daten der Kanzlei außerhalb der Auftragsverarbeitung auch für Produktverbesserungszwecke, Zwecke anderer Kunden, Zwecke von Konzernunternehmen, Marketingzwecke etc. verwendet (ggf. nach Anonymisierung).

4. **Berufsgeheimnis vs. US Cloud Act und ähnliche Herausgabepflichten an Behörden ausländischer Staaten:** Der Dienstanbieter muss transparent machen und sich verpflichten, dass er Anfragen ausländischer Behörden, die auf Daten der Kanzlei zugreifen wollen, verweigert und dass er solche Behörden direkt an den jeweiligen Kunden (also an die Kanzlei) verweist. Auch US-Anbieter verpflichten sich teilweise, gegen Herausgabeverlangen ausländischer Behörden im Hinblick auf Daten ihrer Kunden, die Berufsgeheimnisträger sind, alle zumutbaren rechtlichen und prozessualen Schritte zu unternehmen und solche Daten allenfalls auf Grundlage eines internationalen Durchsuchungsbeschlusses herauszugeben. In solchen Fällen verpflichtet sich der Anbieter, die Kanzlei unverzüglich zu informieren. Ob dies den Anforderungen von § 203 StGB, § 43 e BRAO, § 2 BORA genügt, bleibt abzuwarten.

5. **Verschlüsselungskonzept:** Dieses ist abhängig von der Art der Daten/Vertraulichkeitsstufe der Gesprächsinhalte und bei Berufsgeheimnisträgern ein wichtiger Prüfungspunkt bei der Auswahlentscheidung. Zu unterscheiden ist zwischen der Transportverschlüsselung und der Ende-zu-Ende-Verschlüsselung. Erstere ist üblich. Vorzugswürdig gerade für Berufsgeheimnisträger sind Webconferencing-Lösungen, bei denen die Inhalte der Videokonferenz und der ausgetauschten Chatdaten und Dateien sowie die Nutzungsdaten (inkl. Authentifizierungsdaten der Meeting-Teilnehmer) gegenüber externen Dienstanbietern verschlüsselt sind und auch das Schlüssel-Management entsprechend eingerichtet ist. Dies dürfte aber nur selten der Fall bzw. technisch möglich sein. Dann liegt der Fokus auf kurzen Löschfristen beim Anbieter (siehe 6.). Auch bei Dienstanbietern aus Deutschland oder EU/EWR kommen ggf. Subunternehmer aus Drittländern zum Einsatz (z. B. hinsichtlich der

14 Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, v. 30.3.2020, S. 2.

15 Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, v. 30.3.2020, S. 2.

Cloud-Infrastruktur). In solchen Fällen kann für die datenschutzrechtliche Zulässigkeit (siehe oben 2.) relevant sein, inwieweit der Cloud-Infrastrukturanbieter logisch auf Content/Nutzungsdaten, die beim Dienstanbieter anfallen, zugreifen kann oder ob diese Daten (einschließlich IP-Adressen der Tool-Nutzer) für den Cloud-Anbieter verschlüsselt sind und er auch keinen Zugriff auf die Schlüssel hat.

6. **Löschkonzept:** Die Berliner Datenschutzbehörde[16] hatte in 2016 den Einsatz von Skype für Bewerbungsgespräche einer öffentlichen Stelle u. a. deshalb für unzulässig erachtet, weil nach den damaligen Nutzungsbedingungen von Skype die Chats für 90 Tage auf den Servern von Skype in den USA gespeichert wurden. Inzwischen haben viele Dienstanbieter ihre Bedingungen und Datenschutzerklärungen im Hinblick auf die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO) nachgebessert. Der Diensteanbieter sollte detailliert über seine Regellöschfristen (auch in Datensicherungen) informieren. Auch die Kanzlei als Kunde sollte konkrete Speicherbegrenzungen festlegen. Entsprechende Einstellmöglichkeiten des Tools (default) sind zu nutzen. Das betrifft auch Einstellungen/Abwahl von Funktionen.

7. **Beschränkung von Logfiles:** Bevor sich die Kanzlei für ein Videokonferenzsystem entscheidet, sollte der Dienstanbieter offenlegen, welche Logfiles über die Nutzung des Videokonferenzsystems bei ihm anfallen, erforderlich sind (z. B. zur Fehlerbehebung und um unbefugte Zugriffsversuche auf virtuelle Meeting-Räume zu protokollieren), zu welchen Zwecken die Logfiles gespeichert und ausgewertet werden und welche Regellöschfristen gelten.

8. **Chatverläufe und Dateiaustausch:** Auch für Chat und Dateiaustausch sind Regellöschfristen für eine automatische Löschung beim Dienstanbieter festzulegen. Bei Dateiaustausch kann z. B. ein Zeitraum von wenigen Stunden oder einem Tag gewählt werden, innerhalb dessen die nutzenden Anwälte und Teilnehmer einer Videokonferenz Zeit haben, die Daten herunterzuladen und anderweitig abzulegen oder den Chat ggf. aus berufsrechtlichen Gründen zu dokumentieren.

9. **Audio-/Videoaufzeichnungsfunktion:** Viele Videokonferenzsysteme bieten die Möglichkeit zur Audio-/Videoaufzeichnung. Dies dürfte in den meisten Fällen jedoch nur mit einer Einwilligung aller Teilnehmer zulässig sein. Daher sollte das System so eingestellt werden können und eingestellt sein, dass vor Start der Aufnahme bei allen Teilnehmern eine Nachricht mit den nötigen Informationen erscheint sowie die Option, zuzustimmen oder abzulehnen. Aufzeichnungen ohne wirksame Einwilligung können strafbar sein und für eine weitere Verarbeitung von Bildern (Videos) ist im Regelfall nicht nur aus datenschutzrechtlichen Gründen eine Rechtsgrundlage erforderlich (Stichwort: Kunsturhebergesetz[17]).

10. **Blurr-Funktion:** Manche Videokonferenz-Tools bieten die Funktion, den realen Hintergrund des Meeting-Teilnehmers z. B. durch Bilder fiktiver Räume zu ersetzen. Gerade für Beschäftigte im Homeoffice ist das eine empfehlenswerte technische Maßnahme und gemäß Art. 25 DSGVO geboten.

11. **Einweisung der nutzenden Anwälte und Arbeitsanweisung:** Alle nutzenden Anwälte sind rechtzeitig zu informieren und zu sensibilisieren, welche Daten über das Videokonferenzsystem geteilt bzw. mitgeteilt werden dürfen. Als interne organisatorische Maßnahme in der Kanzlei ist eine Arbeitsanweisung (z. B. als Blacklist) sinnvoll.

12. **Desktop-Sharing-Funktion:** Gerade insoweit empfiehlt sich eine Schulung der nutzenden Anwälte. Z. B. sollten keine Benachrichtigungen über neue Mails auf einem mit anderen Meeting-Teilnehmern geteilten Bildschirm erscheinen. Entweder kann dies grundsätzlich oder für die jeweilige Konferenz unterbunden werden. Meeting-Teilnehmer, die gleichzeitig mehrere Monitore verwenden, müssen entsprechend sorgfältig auswählen, welchen Bildschirm sie in der Konferenz teilen.

13. **Vor dem Desktop-Sharing Urheberrechte an Dokumenten beachten:** Eingebrachte und gemeinsam diskutierte und bearbeitete Dokumente genießen evtl. urheberrechtlichen Schutz, möglicherweise haben auch Dritte Rechte daran. Es ist zu prüfen bzw. zu beachten, dass weder das Videokonferenzsystem unzulässiger Weise vervielfältigt oder öffentlich verfügbar gemacht wird (siehe auch oben 1.) noch Urheberrechte an den Dokumenten, die mittels des Tools „geteilt" werden, verletzt werden. Werden urheberrechtlich geschützte Dokumente während der Videokonferenz bearbeitet und dann weiter genutzt oder verbreitet, müssen grds. alle Beteiligten über die entsprechenden urheberrechtlichen Rechte verfügen.

14. **Einrichtung von Zugangsbeschränkungen (wie Login, oder bei Gästen nur mit Zustimmung des Organisators/Moderators):** Solche Funktionalitäten sehen die Videokonferenzsysteme im Regelfall vor, aber die nutzenden Anwälte müssen entsprechend eingewiesen und ggf. angewiesen werden. Die Sicherheit und Vertraulichkeit von Videokonferenzen können Funktionalitäten erhöhen, die per Default die Sperrung von Meeting-Räumen von Nutzern z. B. 10 Minuten nach Beginn der Sitzung automatisch erzwingen. Dadurch wird verhindert, dass unerwünschte Personen an Meetings teilnehmen. Wenn Teilnehmer versuchen, einem gesperrten Meeting beizutreten, wird der Moderator darauf hingewiesen, dass diese auf eine Genehmigung warten. Zudem sollte ein Erzwingen von Meeting-Passwörtern beim Beitritt über das Telefon oder über Videokonferenzsysteme eingerichtet und genutzt werden.

Isabell Conrad, Rechtsanwältin, Fachanwältin für IT-Recht, SSW Rechtsanwälte Steuerberater Wirtschaftsprüfer, München, www.ssw.eu

16 Bln BDI, Jahresbericht 2016, S. 116

17 Die Anwendung des KUG im nicht-journalistischen Bereich ist seit Geltung des DSGVO umstritten.