



Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit als Datenschutz-Aufsichtsbehörde wird vor dem Hintergrund der Corona-Pandemie verstärkt hinsichtlich des datenschutzkonformen Einsatzes von Videokonferenzlösungen kontaktiert. Um unserer Aufsicht unterliegenden Verantwortlichen die Prüfung der Rechtmäßigkeit der Nutzung verschiedener Lösungen zu erleichtern, veröffentlichen wir folgend die Ergebnisse der durch uns durchgeführten Kurzprüfungen der Videokonferenzdienste verschiedener Anbieter, wobei wir den Schwerpunkt auf die Bewertung der Rechtskonformität der von den Anbietern angebotenen Auftragsverarbeitungsverträge gelegt haben.

Sofern die Anbieter nach einer Kurzprüfung rechtskonforme Auftragsverarbeitungsverträge bereithalten sowie uns Informationen bzw. einen Test-Zugang zur Verfügung gestellt haben, führten wir zwei weitere Prüfschritte durch. Zum einen suchten wir kursorisch nach Hinweisen, ob die Anbieter Datenexporte in Drittländer vornehmen. Zum anderen prüften wir einige technische Eigenschaften der Dienste, die für die Einhaltung der Datenschutzgrundsätze von Bedeutung sind. Selbstverständlich sind diese technischen Eigenschaften nur dann von Relevanz, wenn die Auftragsverarbeitungsverträge rechtskonform ausfallen und wir keine Hinweise dafür gefunden haben, dass die Anbieter hinsichtlich eingeschalteter Subunternehmer oder dem Ort der Datenverarbeitung von den Festlegungen der Verträge abweichen. Nur die Produkte, die diese grundlegenden Anforderungen erfüllten, wurden anschließend noch der technischen Überprüfung unterzogen.

Die Bewertung erfolgt dementsprechend in zwei Teilen: einerseits rechtlich (Teil 1), andererseits – soweit wir rechtlich zur Zulässigkeit der Nutzung durch Berliner Verantwortliche gelangt sind – technisch (Teil 2). Für die beiden Teile der Bewertung gibt es getrennte Tabellen zur Übersicht.

Betrachtetes Betriebsmodell

Die vorliegende Bewertung erstreckt sich ausschließlich auf Dienste, die Videokonferenzen als Software-as-a-Service (SaaS) anbieten. Aus technischer Sicht ist jedoch diesen Angeboten mit vorkonfigurierten Einstellungen, die in vielen Fällen auch nicht verändert werden können, der Betrieb eines Dienstes durch die Verantwortlichen selbst (ggf. auf einer durch einen Auftragsverarbeiter bereitgestellten Plattform) regelmäßig vorzuziehen, da die Verantwortlichen dann die Umstände der Verarbeitung vollumfänglich selbst bestimmen können. In Abhängigkeit von den Verarbeitungsumständen und den spezifischen Risiken kann dies ggf. auch die einzig verfügbare rechtskonforme Lösung sein.

Teil 1: Gestaltung und Umsetzung des Auftragsverarbeitungsverhältnisses

Die vorliegenden Hinweise legen bei der Bewertung der einzelnen Dienste die Musterverträge zugrunde, die die Dienstleister ihren Kunden zur Erfüllung der Verpflichtung gemäß Art. 28 Abs. 3 DS-GVO anbieten. Allgemeine Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten mit Stand vom 3.7.2020 haben wir unter der Adresse https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BInBDI-Empfehlungen_Pruefung_Auftragsverarbeitungsvertraege_Videokonferenz-Dienste.pdf veröffentlicht.

Soweit rechtliche Mängel in den geprüften Dokumenten vorhanden sind, dürfen die Dienste nur genutzt werden, wenn abweichende Vereinbarungen mit den Anbietern getroffen wurden.

Datenexporte und Zugriffsmöglichkeiten von Behörden in Drittländern

Diese Hinweise berücksichtigen die Anforderungen an Datenexporte in Drittländer, die der Gerichtshof der Europäischen Union (EuGH) in seinem Urteil „Schrems II“ vom 16. Juli 2020 (Rs. C-311/18) aufgestellt hat. Sie berücksichtigen dagegen nicht die möglichen rechtlichen Folgen, sollte es in datenschutzrechtlichen Fragen zu einem so genannten „harten Brexit“ kommen, sollte also das Vereinigte Königreich ab dem 1. April bzw. Juni 2021 als Drittland ohne Sonderregelungen zu behandeln sein, ohne dass ein Angemessenheitsbeschluss der EU-Kommission über das Datenschutzniveau im Vereinigten Königreich vorliegt, oder sollte sich die Vereinbarung, das Vereinigte Königreich datenschutzrechtlich vorübergehend noch wie ein EU-Mitglied zu behandeln, als nichtig erweisen. Sie berücksichtigen ebenfalls nicht die Frage, welche Auswirkungen es hat, wenn der Anbieter eines Videokonferenzdienstes zwar die anfallenden personenbezogenen Daten innerhalb des Europäischen Wirtschaftsraums verarbeitet, aber entweder selbst oder über eine Konzerngesellschaft fremdem Recht unterliegt. Dies könnte im Zusammenhang mit Videokonferenzdiensten insbesondere bei US-amerikanischen Unternehmen oder deren Tochtergesellschaften zu datenschutzrechtlichen Problemen führen, wenn nicht durch zusätzliche Maßnahmen nach europäischem Recht unzulässige Zugriffe ausländischer Behörden verhindert werden (etwa mittels Einschaltung eines nicht fremdem Recht unterliegenden Datentreuhänders, durch die ein Zugriff des Anbieters selbst auf personenbezogene Daten ausgeschlossen wird). Hinweise darauf, dass insoweit nach europäischem Recht unzulässige Zugriffsbefugnisse bestehen könnten, gibt es zwischenzeitlich. So steht bei einem Anbieter einer Bewertung mit „Grün“ auf der rechtlichen Ebene neben unzulässigen Datenexporten nur entgegen, dass der Vertrag weisungswidrige Verarbeitungen personenbezogener Daten nicht nur aus dem Recht der Europäischen Union oder der Mitgliedstaaten zulässt. Insoweit teilte der Anbieter uns ausdrücklich mit, dass man sich als US-Unternehmen in einem Konflikt zwischen Rechtssystemen mit sich widersprechenden Anforderungen befinde, der für das Unternehmen nicht lösbar sei. Berliner Verantwortliche, die Videokonferenzdienste nutzen wollen, deren Anbieter direkt oder indirekt ausländischem Recht unterliegen, müssen daher entsprechende Prüfungen selbst vornehmen und die weiteren Entwicklungen genau beobachten.

Rechtsrahmen für OTT-Dienste

Zum 21. Dezember 2020 hätten die EU-Mitgliedstaaten die Regelungen der EU-Richtlinie zum Telekommunikations-Kodex¹ in nationales Recht umsetzen und anwenden müssen. Dadurch wären sogenannte Over-the-top-Dienste (OTT-Dienste) wie Videokonferenzdienste über das Internet einem neuen Rechtsrahmen unterworfen worden. Da eine fristgerechte Umsetzung in Deutschland nicht erfolgte, gilt die bisherige Rechtslage fort.

¹ Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation.

Bewertungsschema Teil 1 (rechtliche Prüfung)

Für die rechtliche Bewertung der Vertragsdokumente und der von uns beobachteten tatsächlichen Datenverarbeitung haben wir folgendes Bewertungsschema verwendet.

Gesamtnote



Es liegen Mängel vor, die eine rechtskonforme Nutzung des Dienstes ausschließen und deren Beseitigung vermutlich wesentliche Anpassungen der Geschäftsabläufe erfordert, etwa wenn

- nach dem Vertrag der Anbieter die im Auftrag verarbeiteten personenbezogenen Daten auch zu eigenen Zwecken verarbeiten darf,
- der Vertrag Datenlöschungen nur verspätet oder eingeschränkt vorsieht,
- die vertraglichen Anforderungen an die Einbindung von Subunternehmern derzeit nicht ausreichend ausgestaltet sind und voraussichtlich Änderungen in den Verträgen zwischen Anbietern und Subunternehmern erforderlich sind,
- der Vertrag unzulässige Datenexporte vorsieht, die im Rahmen der Nutzung des Dienstes auch nicht vermieden werden können.

Ebenfalls mit „Rot“ bewertet haben wir Dienste, bei denen wir im Vertrag selbst zwar keine Mängel festgestellt haben, die aber nach dem Ergebnis unserer technischen Prüfungen Dienstleister einschalten, die nicht vertraglich als Unterauftragsverarbeiter genehmigt sind, und/oder bei denen Datenexporte erfolgen, die nach dem Vertrag nicht gestattet sind.



Es liegen Mängel vor, die eine rechtskonforme Nutzung des Dienstes zwar ausschließen, deren Beseitigung allerdings vermutlich ohne wesentliche Anpassungen der Geschäftsabläufe möglich ist. Hierunter fallen auch Dienste, die vertraglich unzulässige Datenexporte vorsehen, die jedoch im Rahmen der Nutzung des Dienstes vermieden werden können. (Diese Bewertung wurde in dieser Version nicht vergeben.)



Es wurden bei unserer Kurzprüfung keine Mängel gefunden.

Arten der Mängel

Bei der rechtlichen Bewertung gefundene Mängel haben wir wie folgt gekennzeichnet:

- (v) (Vertrag) → Die geprüften Vertragsdokumente weisen rechtliche Mängel auf.
- (d) (Dienstleister) → In die Erbringung des Videokonferenzdienstes wurden nach unseren Prüfungen des Datenverkehrs Dienstleister einbezogen, die nicht als Unterauftragsverarbeiter genehmigt sind. Die Prüfung auf die Einschaltung nicht gestatteter Dienstleister erfolgt nur dann, wenn die vorgelagerte Prüfung der Vertragsdokumente keine Mängel ergeben hat.
- (e) (Export) → Im Rahmen unserer Prüfungen des Datenverkehrs haben wir nicht vertraglich vorgesehene Datenexporte in Drittländer festgestellt. Die Prüfung auf nicht gestattete Datenexporte erfolgt nur dann, wenn die vorgelagerte Prüfung der Vertragsdokumente keine Mängel ergeben hat.

Eine detaillierte Beschreibung der gefundenen Mängel findet sich in den Anmerkungen zu den einzelnen Anbietern am Ende dieses Papiers.

Ort der Datenverarbeitung/Verzicht auf Datenexporte – Spalte „EU“

- Mit diesem Symbol in der Spalte „EU“ sind diejenigen Dienste gekennzeichnet, bei denen nach dem Vertrag der Ort der Verarbeitung der personenbezogenen Daten auf die Europäische Union bzw. den Europäischen Wirtschaftsraum beschränkt ist. Ist dies nicht der Fall, ist für die damit verbundenen Datenexporte nach Art. 44 ff. DS-GVO eine zusätzliche Rechtfertigung erforderlich. Bei Nichterfüllung wird das Symbol genutzt.

Bewertung Teil 1










Die geprüften Videokonferenzdienste haben wir zur Übersichtlichkeit aus rechtlicher Sicht wie folgt zusammenfassend bewertet (zur technischen Bewertung der hier grün bewerteten Dienste siehe Bewertung Teil 2).

	EU	Dienst	URL	Version der Dokumente
	<input checked="" type="checkbox"/>	A-Confi	https://alstermedia.de/videokonferenz	Anlage 1 AV / Version 14.12.2020 [Deutsch]
	<input checked="" type="checkbox"/>	alfaview	https://alfaview.com	Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO, Stand: Dezember 2020 [Deutsch]
(v)	<input type="checkbox"/>	Cisco Webex Meetings	https://www.webex.com/de	Cisco Master Data Protection Agreement, Version 1.0 – Germany, 1. Dezember 2020 [Englisch]; Digital River Ireland Ltd. Allgemeine Geschäftsbedingungen und Verbraucherinformationen Deutschland vom 24.7.2017 [Deutsch]
(d), (e)	<input type="checkbox"/> ²	Cisco Webex Meetings über Telekom	https://konferenzen.telekom.de/produkte-und-preise/telefon-und-web/cisco-webexr/	Anhang AVV zum Vertrag über Telekommunikationsleistungen mit den Annexen für Cisco Webex – Conferencing und Collaboration Konferenzlösungen, Version 3.0 vom 14.12.2020 [Deutsch]
	<input type="checkbox"/> ³	Cloud1X Meet	https://www.cloud1x.de/meet/	Vertrag zur Auftragsverarbeitung für „Cloud1X Meet powered by Jitsi“ – kurz „Cloud1X Meet“, Version 9 vom 15.12.2020 [Deutsch]
⁴		frei verfügbare Jitsi-Angebote		
(v)	<input type="checkbox"/>	Google Meet (als Teil von Google Workspace unter Geltung des Google Workspace (Online) Agreement und des Data Processing Amendment to Google	https://apps.google.com/meet/	Google Workspace Terms of Service, Last modified: December 21, 2020; Data Processing Amendment to Google Workspace and/or Complimentary Product Agreement, Version 2.3 [Englisch]

² Siehe Anmerkung.

³ Grundsätzlich beschränkt auf EU/EWR, Datenexporte mit vorheriger Zustimmung der/des Verantwortlichen allerdings möglich.








⁴ In der Regel „rot“, da in der Regel kein Auftragsverarbeitungsvertrag. Einzelfallprüfung erforderlich.

	EU	Dienst	URL	Version der Dokumente
		Workspace and/or Complementary Product Agreement)		
 5	<input type="checkbox"/>	Google Meet (kostenlos)	https://apps.google.com/meet/	Google-Nutzungsbedingungen, wirksam ab dem 31. März 2020, Google-Datenschutzerklärung, wirksam ab dem 4. Februar 2021 [Deutsch]
 (v)	<input type="checkbox"/>	GoToMeeting	https://www.gotomeeting.com/de-de	Data Processing Addendum, Revised: December 15, 2020 [Englisch]
	<input checked="" type="checkbox"/>	mailbox.org	https://mailbox.org/video	AV-Vertrag für Kunden von mailbox.org nach Artikel 28 Abs. 3 DS-GVO, Version V.39 vom 15.12.2020 [Deutsch]
	<input type="checkbox"/> 6	meetzi	https://meetzi.de	meetzi – Auftragsverarbeitungs (AV)-Vertrag nach Art. 28 DS-GVO, Version 3 (14.12.2020) [Deutsch]
 (v)	<input type="checkbox"/>	Microsoft Teams (unter Geltung der Online Service Terms, etwa als Teil von Microsoft 365 oder in der kostenfreien Version bei Anmeldung in einer Arbeits- oder Organisationsumgebung)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste Januar 2020 [Deutsch] – Dateiversionen (laut Metadaten) vom 3.1.2020 und 9.6.2020 (Version ist im Dokument selbst nicht ersichtlich); Microsoft-Onlinedienste Nachtrag zum Datenschutz, Letzte Aktualisierung: 21. Juli 2020 [Deutsch]; Additional Safeguards Addendum to Standard Contractual Clauses (Reference Copy gemäß Ankündigung November 2020) [Englisch]; Microsoft Online Services Data Protection Addendum, Last updated December 9, 2020 [Englisch]
 7	<input type="checkbox"/>	Microsoft Teams (kostenlose Version ohne Anwendbarkeit der Online Service Terms, also nicht bei Anmeldung in einer Arbeits- oder Organisationsumgebung)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Microsoft-Servicevertrag gültig ab 1. Oktober 2020, Datenschutzerklärung von Microsoft Letzte Aktualisierung: Januar 2021 [Deutsch]
	<input checked="" type="checkbox"/>	NETWAYS Web Services Jitsi	https://nws.netways.de/apps/jitsi/	AVV v1.7 [Deutsch]
	<input checked="" type="checkbox"/>	OSC BigBlueButton	https://www.open-source-company.de/bigbluebutton-hosting/	Vertrag zur Verarbeitung von personenbezogenen Daten im Auftrag, Version 1.6 (Stand 16.12.2020) [Deutsch]
	<input checked="" type="checkbox"/>	sichere-videokonferenzen z.de	https://sichere-videokonferenz.de	Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung Stand 06/2020 [Deutsch]

⁵ Kein Auftragsverarbeitungsvertrag.

⁶ Grundsätzlich beschränkt auf EU/EWR, Datenexporte mit vorheriger Zustimmung der/des Verantwortlichen allerdings möglich.

⁷ Kein Auftragsverarbeitungsvertrag.

	EU	Dienst	URL	Version der Dokumente
 8	<input type="checkbox"/>	Skype (ohne Anwendbarkeit der Online Service Terms)	https://www.skype.com/de/	Microsoft-Servicevertrag gültig ab 1. Oktober 2020, Datenschutzerklärung von Microsoft November 2020 [Deutsch]
 9	<input type="checkbox"/>	Skype for Business Online (auslaufend, unter Gültigkeit der Online Service Terms)		Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste Januar 2020 [Deutsch] – Dateiversionen (laut Metadaten) vom 3.1.2020 und 9.6.2020 (Version ist im Dokument selbst nicht ersichtlich); Microsoft-Onlinedienste Nachtrag zum Datenschutz, Letzte Aktualisierung: 21. Juli 2020 [Deutsch]; Additional Safeguards Addendum to Standard Contractual Clauses (Reference Copy gemäß Ankündigung November 2020) [Englisch]; Microsoft Online Services Data Protection Addendum, Last updated December 9, 2020 [Englisch]
 (v)	<input type="checkbox"/>	TeamViewer Meeting (ehemals Blizz)	https://www.teamviewer.com/de/meeting/	TeamViewer Auftragsverarbeitungsvertrag (AVV), Versionsstand: 1. Januar 2021; TeamViewer Endbenutzer-Lizenzvereinbarung (EULA), Versionsstand: 1. Januar 2021; TeamViewer Produkt-Datenschutzrichtlinie“ (ohne Versionsnummer, Abruf 4. Februar 2021) [Deutsch]
	<input checked="" type="checkbox"/>	TixeoCloud	https://www.tixeo.com	Vertrag zur Auftragsverarbeitung Version 20200608 [Deutsch]
	<input checked="" type="checkbox"/>	Werk21 BigBlueButton	https://www.werk21.de/produkte/co_working/bigbluebutton/index.html	Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO, Version 1.2.1., 06/2020 [Deutsch]
	<input type="checkbox"/> 10	Wire Pro	https://wire.com/de/	Datenverarbeitungszusatz Juni 2020 [Deutsch]
 (v)	<input type="checkbox"/>	Zoom	https://zoom.us	Global Data Processing Addendum December 2020 [Englisch]; Zoom Privacy Statement (letzte Änderung August 2020) [Englisch]

⁸ Kein Auftragsverarbeitungsvertrag.

⁹ Siehe Anmerkungen zu Microsoft Teams (unter Geltung der Online Service Terms, etwa als Teil von Microsoft 365 oder in der kostenfreien Version bei Anmeldung in einer Arbeits- oder Organisationsumgebung).

¹⁰ Auch Schweiz. Für die Schweiz besteht ein Angemessenheitsbeschluss der EU-Kommission über das Datenschutzniveau.

Teil 2: Technische und organisatorische Maßnahmen

Im vorliegenden Abschnitt sind die Ergebnisse unserer Prüfung der Einhaltung der Vorgaben zur Datensicherheit sowie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art. 25 und 32 DS-GVO hinsichtlich der Dienste wiedergegeben, die sich nicht bereits in der rechtlichen Prüfung als unzulässig erwiesen haben.

Anwendungsfall und Annahmen

Für die Kurzprüfung sind wir von einigen grundsätzlichen Annahmen ausgegangen. Diese beziehen sich zum einen auf das grundsätzliche Vorgehen bei der Anwendung der Dienste und zum anderen auf mehrere typische Anwendungsfälle, die sich durch den Schutzbedarf der Verarbeitung unterscheiden.

Annahmen zu den Anwendungsfällen

Wir haben vier typische Anwendungsfälle zu Grunde gelegt, bei denen eine Konferenz durch eine Person organisiert wird, die eine weitere Person oder Personengruppe als weitere Teilnehmende bestimmt und durch eine Einladung zur Teilnahme an der Konferenz autorisiert.

Von einer solchen Konferenz erwarten die teilnehmenden Personen, dass die Kommunikationsinhalte nur zwischen den autorisierten Personen geteilt und hinterher nicht gespeichert und für andere Zwecke genutzt werden, es sei denn, es gibt für Speicherung und Weiterverarbeitung eine Rechtsgrundlage und die Teilnehmenden werden vorab informiert. Des Weiteren erwarten sie, dass sie Ton und Bild ihrer Eingabegeräte selbst steuern können und eine Aktivierung, beispielsweise durch Moderator*innen oder Dritte aus der Ferne, ohne die Mitwirkung der Teilnehmenden selbst ausgeschlossen ist.

In Bezug auf die genutzte Informationstechnik wird für die Bewertung vorausgesetzt, dass die Dienstleistung vollständig durch den Auftragsverarbeiter ohne Verknüpfung mit internen Diensten der Verantwortlichen erbracht wird und im Zusammenhang mit den Konferenzen auch keine von dem Dienst unabhängigen weiteren Auftragsverarbeiter in Anspruch genommen werden. Insbesondere kommt kein Authentifizierungsdienst zum Einsatz, der durch die Verantwortlichen oder nicht an der Erbringung des Videokonferenzdienstes beteiligte Dritte bereitgestellt wird.

In Bezug auf die Inhalte der Konferenz wird vorausgesetzt, dass eine Rechtsgrundlage für ihre Übermittlung mit den verschiedenen Funktionalitäten des Dienstes besteht, sodass eine Unterbindung dieser Funktionalitäten nicht erforderlich ist.

Anwendungsfall 1: Geringfügige Risiken

In diesem Anwendungsfall erwachsen den teilnehmenden Personen aus der Teilnahme an der Konferenz (einschließlich ihrer Äußerungen) nur Risiken geringfügiger Schwere. Insbesondere führt eine unbefugte Offenlegung oder Veränderung von Daten über diese Teilnahme nicht zu mehr als geringfügigen Folgen.

Es werden durch den Verantwortlichen keine Aufzeichnungen von Ton oder Bild aus der Konferenz vorgenommen, sodass hieraus auch keine Risiken erwachsen können. Unbefugte Aufzeichnungen durch Konferenzteilnehmer*innen, die sich durch technische Maßnahmen nicht ausschließen lassen, bleiben außer Betracht.

Darüber hinaus werden in der Konferenz entweder überhaupt keine Inhalte besprochen, die personenbezogene Daten darstellen, oder unter den Inhalten sind allenfalls beiläufig personenbezogene Daten mit geringfügiger Aussagekraft enthalten, deren unbefugtes Bekanntwerden nur geringfügige Risiken für die betroffenen Personen mit sich bringt.

Anwendungsfall 2: Normal schutzbedürftige Inhalte, Gastteilnahme mit geringfügigen Risiken

In diesem Anwendungsfall wird für die Bewertung ein normaler Schutzbedarf der Inhaltsdaten vorausgesetzt. Dies impliziert, dass von normalen, nicht aber geringfügigen Vertraulichkeitsrisiken ausgegangen wird.

Die Teilnehmenden authentifizieren sich gegenüber dem Videokonferenzdienst mit einem oder mehreren individuellen Merkmalen (typischerweise mit Nutzernamen und Passwort) oder nutzen als Gäste einen Link und ein zusätzliches konferenzspezifisches Passwort.

Im letzteren Fall sorgt die Konferenzmoderation dafür, dass Personen, die unbefugt teilnehmen, erkannt und ausgeschlossen werden.¹¹ Das Risiko, das mit der Konferenzteilnahme Unbefugter bis zu ihrem Ausschluss durch die Moderation verbunden ist, ist geringfügig. Ein späteres Beitreten Unbefugter mit dem Risiko, dass Konferenzinhalte zur Kenntnis genommen werden können, wird technisch verhindert.

Eine Aufzeichnung der Videokonferenz wird nicht durchgängig für alle Videokonferenzen benötigt.

Anwendungsfall 3: Normale Risiken

Dieser Anwendungsfall unterscheidet sich von dem vorigen darin, dass sich die Risiken auch auf die Rahmendaten über die Teilnehmenden und die Umstände der Konferenz erstrecken und das Risiko, das mit der Konferenzteilnahme Unbefugter bis zu ihrem Ausschluss durch die Moderation verbunden ist, mehr als geringfügig ist.

Dies hat als Konsequenz, dass der Kreis der Konferenzteilnehmer*innen vorab festgelegt werden muss und sich die Teilnehmenden mit einem oder mehreren personenindividuellen Merkmalen (typischerweise mit Nutzernamen und Passwort) anmelden müssen.

Anwendungsfall 4: Hohe Risiken

Anwendungsfälle, bei denen schwerwiegende nachteilige Folgen für die betroffenen Personen eintreten können, bedürfen einer individuellen Risikobetrachtung, sodass wir diesbezüglich hier keine pauschale Bewertung der Dienste vornehmen können.

Regelmäßig ist jedoch in diesem Anwendungsfall neben der Vornahme einer Zwei-Faktor-Authentifizierung der Teilnehmenden die Vornahme einer Ende-zu-Ende-Verschlüsselung der Inhaltsdaten zwischen den Konferenzbeteiligten erforderlich, die so ausgestaltet ist, dass der Diensteanbieter die Konferenzinhalte nicht zur Kenntnis nehmen kann, jedenfalls nicht ohne die von den Teilnehmenden eingesetzte Software zu manipulieren.

Wir geben daher in der Zusammenfassung des Ergebnisses an, ob ein Dienst eine Ende-zu-Ende-Verschlüsselung anbietet, und welche Qualität sie ggf. aufweist.

Hierbei unterscheiden wir zwischen einer starken und einer schwachen Variante. Der Unterschied besteht darin, dass sich bei der starken Variante die teilnehmenden Endgeräte gegenseitig nachprüfbar authentifizieren lassen und für jede Konferenz neue flüchtige Verschlüsselungsschlüssel unter Kontrolle der Konferenzteilnehmer*innen so erzeugt, ausgehandelt bzw. verteilt werden, dass dem Anbieter keine Kenntnisnahme des Schlüsselmaterials möglich ist.¹² Die schwache Variante der Ende-zu-Ende-Verschlüsselung schützt dagegen davor, dass Beschäftigte des Diensteanbieters die Konferenzinhalte beiläufig zur Kenntnis nehmen, wenn sie durch die Systeme des Diensteanbieters geleitet werden. Sie schützt nicht gegen einen Eingriff

¹¹ Genauere Anforderungen an die Gastteilnahme sind in Nr. 4.2.4 der „Orientierungshilfe Videokonferenzsysteme“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu finden. Verantwortliche sollten zudem darauf achten, die konferenzspezifischen Passwörter nicht wiederzuverwenden, um das Risiko unautorisiert teilnehmender Personen zu reduzieren.

¹² Siehe Kapitel 4.1 der „Orientierungshilfe Videokonferenzsysteme“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK).

des Diensteanbieters in die Datenverarbeitung der von ihm betriebenen Systeme, der auf eine Ausleitung der Konferenzinhalte gerichtet ist. Eine korrekt eingesetzte starke Ende-zu-Ende-Verschlüsselung schützt auch gegen einen solchen Eingriff.

Prüfkriterien

Als technische Prüfkriterien wurden die Anforderungen an technische und organisatorische Maßnahmen in Kapitel 4 der „Orientierungshilfe Videokonferenzsysteme“¹³ (OH VK) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) herangezogen. Nur diejenigen Maßnahmen wurden überprüft, die sich durch Untersuchung und Test des auf Nutzerseite eingesetzten Client-Programms beurteilen lassen.

Die Prüfkriterien waren damit:

Prüfkriterium	Verweis auf OH VK
Für die Übertragung der Videokonferenzdaten werden mindestens Transportverschlüsselungen nach dem Stand der Technik genutzt.	4.1
Der Videokonferenzdienst bietet die Möglichkeit, die Teilnahme an einer Konferenz auf Personen zu beschränken, die sich mit individuellen Merkmalen angemeldet haben. ¹⁴	4.2
<i>Für Anwendungsfall 1 und 2 alternativ zum vorigen Kriterium:</i> Der Videokonferenzdienst bietet einer durch den Verantwortlichen bestimmten Person in der Moderationsrolle die Möglichkeit, nicht zur Teilnahme an der Konferenz autorisierte Personen zu erkennen und aktiv derart auszuschließen, dass ein erneuter Eintritt in die Konferenz nicht möglich ist.	4.2.4
Das Videokonferenzsystem ermöglicht die Einrichtung von Rollen für administrierende, moderierende, präsentierende und teilnehmende Personen. Andere Rollenzuschnitte sind möglich, soweit die Verantwortung für die Steuerung der implizit vorgenommenen Verarbeitung von personenbezogenen Daten klar zugewiesen bleibt.	4.4
Die teilnehmenden Personen können ihr Mikrofon und ihre Kamera jederzeit deaktivieren. Ohne die Zustimmung der teilnehmenden Person können deren Mikrofon und deren Kamera nicht aktiviert werden.	4.4
Die Clientsoftware übermittelt keine Daten an den Diensteanbieter, die der Auswertung der Nutzung des Dienstes durch den Diensteanbieter oder Dritte dienen (Tracking).	4.5
Vor Eintritt in die Konferenz sind Funktionen von Kamera und Mikrofon und das Teilen des Bildschirms deaktiviert und müssen erst von der teilnehmenden Person aktiviert werden.	4.5
(Systemseitige) Aufzeichnungen können unterbunden werden.	4.7

¹³ https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf.

¹⁴ Ob das Authentifizierungsverfahren dem Stand der Technik entspricht (vgl. Kapitel 4.2.1 der Orientierungshilfe Videokonferenzsysteme), konnten wir nicht bei allen Anbietern überprüfen. Aus Gründen der Gleichbehandlung ist dieser Aspekt daher nicht Gegenstand der Bewertung. Wir führen unsere diesbezüglichen Feststellungen zu einigen Anbietern daher nur informationshalber in den Anmerkungen auf.

Prüfkriterium	Verweis auf OH VK
Alle teilnehmenden Personen werden durch einen expliziten und durch die teilnehmende Person zu bestätigenden Hinweis oder durch Kennzeichnung innerhalb der Benutzerschnittstelle darauf hingewiesen, dass die Videokonferenz ganz oder in Teilen aufgezeichnet wird.	4.7

Nicht geprüft wurden folgende Aspekte:

- Maßnahmen zum Datenschutz durch Technikgestaltung, insbesondere zur Datensparsamkeit und Speicherbegrenzung bei der Verarbeitung von Rahmen-¹⁵ und Inhaltsdaten durch den Anbieter, einschließlich der unverzüglichen automatisierten Löschung von personenbezogenen Rahmen- und Inhaltsdaten durch den Anbieter nach Ende der Videokonferenz oder des Bestehens einer Möglichkeit für die Verantwortlichen, eine solche Löschung zu bewirken,
- Umfang und Korrektheit der Angaben der Anbieter über ihre Verarbeitung von personenbezogenen Rahmendaten (z. B. aus der Einrichtung der Konferenz oder der Inanspruchnahme von Funktionen des Dienstes),
- das Bestehen einer Möglichkeit zur Einbindung von Informationen gemäß Art. 13 bzw. 14 DS-GVO in die Client-Software,
- der Ausschluss der Offenlegung von personenbezogenen Daten aus der Dienstbringung durch die Anbieter des Dienstes an Dritte, die nicht an der Erbringung des Dienstes beteiligt sind, wie z. B. die Hersteller der Software, die von den Diensteanbietern eingesetzt wird,
- die Eignung des durch den Anbieter vorbereiteten Berechtigungskonzepts [soweit der Anbieter teilnehmenden Personen, die nicht zu den Organisator*innen der Konferenz gehören, keine individuelle Authentifizierung ermöglicht, wurde jedoch das Vorhandensein einer Funktion zum Ausschluss von unerwünschten Teilnehmenden durch eine hierzu befugte Person (Organisator*in, Moderator*in) geprüft],
- das Vorhandensein von bekannten Schwachstellen in den Software-Bibliotheken der Client-Programme und in den zur Bereitstellung der Dienste genutzten Web-Anwendungen.

Die Ergebnisse der Untersuchungen haben wir am Ende dieses Papiers in den Anmerkungen zu den einzelnen Anbietern zusammengefasst, um es den Verantwortlichen zu erleichtern, einen für ihre Zwecke geeigneten Dienst auszuwählen und, soweit erforderlich, ergänzende technische und organisatorische Maßnahmen zu ergreifen.

Anpassung an den Anwendungskontext

Vor dem Einsatz müssen Verantwortliche den Anwendungskontext und die konkreten Anwendungsfälle betrachten, um eine angemessene Risikoabschätzung durchführen und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen festlegen zu können. Insbesondere ist es möglich, dass aufgrund der vorliegenden Risiken zusätzliche Maßnahmen ergriffen werden müssen, die jedoch durch den Anbieter nicht unterstützt werden, ohne dass wir dies als Mangel vermerkt haben. Verantwortliche müssen in dem letztgenannten Fall überprüfen, ob sie den Mangel durch eigene Maßnahmen kompensieren können oder einen anderen Anbieter wählen müssen.

Zu diesen risikobezogenen Maßnahmen kann es insbesondere gehören, sich der Identität der Teilnehmenden der Konferenz und der Sicherheit der Verbindung zu versichern, wenn

¹⁵ Rahmendaten sind Metadaten über die Durchführung der Kommunikation. Sie können z. B. Informationen über berufliche Kontakte, Arbeitszeiten oder Arbeitsleistung enthalten.

der gewählte Dienst hierfür nur Mechanismen bereithält, die in Anbetracht des Schutzbedarfs der Kommunikationsinhalte nicht ausreichend sind.

Weitere nützliche Hinweise zur datenschutzgerechten Konfiguration und Nutzung von Videokonferenzdiensten sind insbesondere der bereits zitierten Orientierungshilfe Videokonferenzsysteme der DSK sowie unseren Veröffentlichungen „Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen“¹⁶ und „Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen“¹⁷ zu entnehmen.

Bewertungsschema Teil 2 (technische Prüfung)

Für die technische Bewertung der Dienste haben wir folgendes Bewertungsschema verwendet.

Gesamtnote



Es liegen schwerwiegende Mängel vor, die eine rechtskonforme Nutzung des Dienstes im Rahmen des geprüften Anwendungsfalls ausschließen.



Es liegen Mängel vor, die im Rahmen des jeweiligen Anwendungsfalls zu einer Verletzung der datenschutzrechtlichen Anforderungen gemäß Art. 25 oder 32 DS-GVO führen können. Die Eintrittswahrscheinlichkeit der mit der Nutzung des Dienstes verbundenen Risiken hängt von der Vornahme ergänzender Maßnahmen durch die Verantwortlichen ab, die Schwere dieser Risiken vom jeweiligen Anwendungsfall. Hält sich das Restrisiko nicht in einem angemessenen Rahmen, kann der Dienst nicht rechtskonform eingesetzt werden.



Im Rahmen unserer Untersuchung gemäß der dargestellten Prüfkriterien haben wir keine Anhaltspunkte für Mängel mit Relevanz für den jeweiligen Anwendungsfall gefunden.

Ein Dienst weist dann einen Mangel auf, wenn es den Verantwortlichen durch Nutzung der durch den Anbieter angebotenen Konfigurationsoptionen nicht möglich ist, eine rechtskonforme Datenverarbeitung zu gewährleisten.

Arten der vorgefundenen Mängel

Im Rahmen der oben aufgeführten technischen Prüfkriterien konnten wir bei den von uns geprüften Diensten lediglich drei Mängel feststellen, die eine positive Bewertung verhindern. Wir haben sie mit den Buchstaben (a), (r) und (k) gekennzeichnet.

- (a) (Anmeldung) → Der Dienst erlaubt es nicht, die Teilnehmenden zu verpflichten, sich mit individuellen Merkmalen (typischerweise Nutzernamen und Passwort) anzumelden (Nr. 4.2 der Orientierungshilfe Videokonferenzsysteme, siehe Erläuterung oben unter Prüfkriterien).
- (r) (Rollenkonzept) → Der Dienst erlaubt keine Umsetzung eines Rollenkonzepts gemäß Nr. 4.4 der Orientierungshilfe Videokonferenzsysteme (siehe Erläuterung oben unter Prüfkriterien).
- (k) (Kamera) → Den Teilnehmenden ist es bei dem betreffenden Dienst nicht möglich, mit deaktivierter Kamera und deaktiviertem Mikrofon einer Konferenz beizutreten

¹⁶ https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BInBDI-Empfehlungen_Videokonferenzsysteme.pdf.

¹⁷ https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BInBDI-Checkliste_Videokonferenzen.pdf.

(Nr. 4.5 der Orientierungshilfe Videokonferenzsysteme, siehe Erläuterung oben unter Prüfkriterien).

Bei der Anwendung des fraglichen Dienstes wird der mit (k) bezeichnete Umstand regelmäßig, aber nicht stets zu einem Verstoß gegen Art. 25 DS-GVO führen – dies hängt von den Umständen des Einzelfalls ab. Beispielsweise bei Videokonferenzen zwischen zwei Personen wird hier regelmäßig nicht von einem Verstoß gegen Art. 25 DS-GVO auszugehen sein.

Eine detaillierte Beschreibung der gefundenen Mängel findet sich in den Anmerkungen zu den einzelnen Anbietern am Ende dieses Papiers.

Zur angemessenen Einordnung der Ergebnisse möchten wir darauf hinweisen, dass durch unzureichende technisch-organisatorische Maßnahmen im Backend der Dienste und Schwachstellen der Client-Software noch weit gravierendere Mängel entstehen können als durch unsere Tests feststellbar waren.

Ende-zu-Ende-Verschlüsselung – Spalte E2E

- + Mit dem Plus-Symbol sind die Dienste gekennzeichnet, die eine im oben erläuterten Sinn schwache Ende-zu-Ende-Verschlüsselung anbieten.
- ++ Mit zwei Plus-Symbolen ist eine starke Ende-zu-Ende-Verschlüsselung markiert.

Bewertung Teil 2

Die geprüften Videokonferenzdienste haben wir zur Übersichtlichkeit aus technischer Sicht wie folgt zusammenfassend bewertet (zur rechtlichen Bewertung siehe Bewertung Teil 1). Anwendungsfall 4 erfordert eine Bewertung im Einzelfall und ist nicht als Ampel darstellbar.

Anwendungsfall ¹⁸			E2E	Dienst	URL
AF1	AF 2	AF 3			
		(a)	+	A-Confi	https://alstermedia.de/videokonferenz
				alfaview	https://alfaview.com
		(a)		Cloud1X Meet	https://www.cloud1x.de/meet/
		(a)		mailbox.org	https://mailbox.org/video
		(a)		meetzi	https://meetzi.de
		(a)		NETWAYS Web Services Jitsi	https://nws.netways.de/de/apps/jitsi/

¹⁸ Die Anwendungsfälle (AF) sind hier wie am Anfang des Kapitels nummeriert.

Anwendungsfall ¹⁸					
AF1	AF 2	AF 3	E2E	Dienst	URL
				OSC BigBlueButton	https://www.open-source-company.de/bigbluebutton-hosting/
				sichere-videokonferenz.de	https://sichere-videokonferenz.de
			+	TixeoCloud	https://www.tixeo.com
				Werk21 BigBlueButton	https://www.werk21.de/produkte/co_working/bigbluebutton/index.html
			++	Wire Pro	https://wire.com/de/

Nur bei dem Dienst Wire Pro haben wir im Anwendungsfall 3 im Hinblick auf die oben aufgeführten Prüfkriterien *bereits in der Standardkonfiguration* keine Anhaltspunkte für Mängel und keine Umstände gefunden, die eine Anpassung der Konfiguration oder zusätzliche Maßnahmen erforderlich machen.

¹⁹ Anbieter hat für Mitte Februar 2021 eine neue Version 16.5 der Software angekündigt, in der die Mängel beseitigt sein sollen.

Teil 3: Anmerkungen zu den einzelnen Anbietern

Bitte beachten Sie, dass es über die hier angesprochenen Fragestellungen hinaus weitere, nicht von uns geprüfte oder uns nicht bekannte Probleme geben und die Nutzung der Dienste dann ggf. trotz Behebung der hier genannten Probleme dennoch unzulässig sein kann.

In *kursiv* haben wir den Anmerkungen eine knappe Zusammenfassung der gefundenen rechtlichen Mängel vorangestellt.

Allgemeine Anmerkungen zu Jitsi Meet

Bei Jitsi Meet handelt es sich um freie und quelloffene Software. Wir haben beispielhaft die Angebote einiger Dienstleister betrachtet, die den Betrieb der Software für Verantwortliche zum Inhalt haben. Hierbei haben die Dienstleister die Software teilweise angepasst. Am Markt sind eine Reihe weiterer Betreiber dieser Software tätig. Mit der Nennung der Anbieter ist keine Aussage dahingehend verbunden, dass ihre Dienstleistung der anderer im Wettbewerb stehender Unternehmen vorzuziehen ist.

Die Bereitstellung eines Jitsi-Systems führt allerdings auch regelmäßig zur Übernahme von technischen Einschränkungen, die sich auf einen datenschutzkonformen Einsatz auswirken und bei den entsprechenden Anbietern systematisch wiederfinden lassen. Einige dieser Einschränkungen können in Abhängigkeit von der Nutzung des Systems dazu führen, dass nicht alle datenschutzrechtlichen Anforderungen erfüllt werden. Um dies zu korrigieren, sind u. U. Anpassungen des Quellcodes der Software notwendig. Eine Übernahme in die öffentlich verfügbare Community-Code-Basis würde es auch anderen Stellen, die die Software einsetzen, ermöglichen, von den Anpassungen zu profitieren.

Eingeschränkt sind insbesondere das Rollenkonzept und die zur Verfügung stehenden Methoden zur Zugangskontrolle.

Außer in Anwendungsfällen mit geringfügigen Risiken sollten die Verantwortlichen darauf achten, dass der von ihnen genutzte Dienst eine Moderationsrolle anbietet, die nur nach Anmeldung mit personenindividuellen Merkmalen (typischerweise mit Nutzernamen und Passwort) übernommen werden kann. Viele Jitsi-Instanzen vergeben die Moderationsrolle an die erste Person, die einen Konferenzraum betritt. Dies ist für Anwendungsfälle mit mehr als geringfügigen Risiken nicht geeignet.

Die uns bekannten Dienste, die Jitsi Meet einsetzen, erlauben es nicht, die Teilnahme an einer Konferenz auf Personen einzuschränken, die sich mit personenindividuellen Merkmalen (typischerweise mit Nutzernamen und Passwort) angemeldet haben. In Abhängigkeit von den weiteren Maßnahmen, die die/der Verantwortliche trifft, und den Risiken im konkreten Anwendungsfall kann dies zur Unzulässigkeit des Einsatzes führen.

Die Anbieter von jitsi-basierten Diensten stellen keine eigenen mobilen Anwendungen (Apps) zur Nutzung ihrer Dienste bereit. Stattdessen können die für alle solche Dienste allgemein einsetzbaren Apps eingesetzt werden. Wir warnen dabei vor der Nutzung der Apps aus dem Google Play Store und dem Apple App Store, die jeweils Software von Tracking-Anbietern wie Crashlytics und Firebase enthalten. Die Variante der Jitsi-App aus dem F-Droid-Store²⁰ dagegen ist frei von derartigen Komponenten. Verantwortliche müssen in der Einladung zu einer Konferenz auf die genannten Defizite der Apps hinweisen und den Zugang zu dem Dienst über die F-Droid-App oder einen Webbrowser empfehlen, soweit diese Information den Eingeladenen noch nicht bekannt ist.

Wie bei jedem Dienst, bei dem es zur Teilnahme an einer Konferenz ausreicht, den Konferenzlink aufzurufen und das Konferenz-Passwort einzugeben, müssen Verantwortliche besonderes Augenmerk auf die Vertraulichkeit der Übergabe des Links zur Konferenz und des

²⁰ <https://f-droid.org>.

Konferenz-Passworts legen. Ein Sicherheitsgewinn kann erzielt werden, indem Passwort und Einladungslink den Teilnehmenden auf unterschiedlichen Kommunikationskanälen mitgeteilt werden.

Allgemeine Anmerkungen zu BigBlueButton

Bei BigBlueButton handelt es sich auch um freie und quelloffene Software. Wir haben beispielhaft die Angebote einiger Dienstleister betrachtet, die den Betrieb der Software für Verantwortliche zum Inhalt haben. Hierbei haben die Dienstleister die Software teilweise angepasst. Am Markt sind eine Reihe weiterer Betreiber dieser Software tätig. Mit der Nennung der Anbieter ist keine Aussage dahingehend verbunden, dass ihre Dienstleistung der anderer im Wettbewerb stehender Unternehmen vorzuziehen ist.

Auch die Bereitstellung eines BigBlueButton-Systems führt regelmäßig zur Übernahme von technischen Einschränkungen, die sich auf einen datenschutzkonformen Einsatz auswirken und sich bei den entsprechenden Anbietern systematisch wiederfinden lassen. Einige dieser Einschränkungen können in Abhängigkeit von der Nutzung des Systems dazu führen, dass nicht alle datenschutzrechtlichen Anforderungen erfüllt werden. Um dies zu korrigieren, sind u. U. Anpassungen des Quellcodes der Software notwendig. Eine Übernahme in die öffentlich verfügbare Community-Code-Basis würde es auch anderen Stellen, die die Software einsetzen, ermöglichen, von den Anpassungen zu profitieren.

Eine derartige technische Einschränkung besteht in der Umsetzung der Aufnahmefunktion für Videokonferenzen. Zum Prüfzeitpunkt sah die offizielle Version der Software vor, dass stets eine Aufnahme der gesamten Konferenz vorgenommen und diese Aufnahme zu einem späteren Zeitpunkt anhand von Schnittmarken zurechtgeschnitten wird. Dies kann zur Unrechtmäßigkeit der Verarbeitung führen und widerspricht in jedem Fall dem Grundsatz der Datenminimierung sowie regelmäßig den Erwartungen der nutzenden Personen. Ein untersuchter Dienst hat daher diese Funktion derart modifiziert, dass sie nach eigener Angabe nun nur noch Aufnahmen für diejenigen Zeitabschnitte speichert, für die dies explizit angefordert wurde.

A-Confi – Jitsi

In der Standardkonfiguration sind Konferenzen dieses Anbieters nicht durch Passwort geschützt. Verantwortliche sollten daher vor dem Starttermin und bevor andere Teilnehmende die Konferenz betreten, die Konferenz eröffnen und ein Passwort setzen.

Um eine teilnehmende Person dauerhaft von der Konferenz auszuschließen, ist es der moderierenden Person möglich, ein neues Passwort zu setzen und die Funktion „Hinauswerfen“ auf die Person anzuwenden.

Im Zuge der Authentifizierung von Personen, die die Moderationsrolle übernehmen, wird entsprechend dem Stand der Technik die Übertragung ihres Passworts an den Anbieter vermieden.

A-Confi bietet eine schwache Variante der Ende-zu-Ende-Verschlüsselung an. Dabei handelt es sich um ein experimentelles Feature von Jitsi.

alfaview

Für das Angebot von alfaview ist die Nutzung einer App erforderlich, die jedoch ohne Administrationsrechte installiert werden kann. Die Desktop-App ist für Windows, MacOS und Linux auf der Webseite von alfaview erhältlich und darf von keiner anderen Quelle heruntergeladen werden. Es muss zudem berücksichtigt werden, ob eine Installation von Software in der intendierten Umgebung möglich ist.

Bei der Transportverschlüsselung haben wir keine Mängel festgestellt. Eine Ende-zu-Ende-Verschlüsselung bietet alfaview nicht an.

Cisco Webex Meetings

Bei Online-Bestellung muss Auftragsverarbeitungsvertrag gesondert abgeschlossen werden. Verarbeitungen ohne Weisung auch aus drittstaatlichem Recht zulässig. Keine ausreichenden ergänzenden Maßnahmen für Datenexporte.

Cisco Webex Meetings kann nicht nur direkt bei Cisco oder über Cisco-Partner (mit Auftragsverarbeitungsvertrag) bezogen werden, sondern auch online. Standardmäßig wird bei der Online-Buchung kein Auftragsverarbeitungsvertrag geschlossen, sodass dies nachgeholt werden muss.

Der Anbieter hat zwar erhebliche Anstrengungen vorgenommen, die Haupt-Verarbeitungen personenbezogener Daten im Zusammenhang mit der Nutzung von Cisco Webex Meetings verstärkt in die EU zu verlagern und den Auftragsverarbeitungsvertrag mangelfrei zu gestalten. Einer Bewertung des Auftragsverarbeitungsvertrags als mangelfrei steht auf der rechtlichen Ebene allerdings bereits entgegen, dass der Vertrag weisungswidrige Verarbeitungen personenbezogener Daten nicht nur aus dem Recht der Europäischen Union oder der Mitgliedstaaten zulässt. Es bleibt letztlich das Problem von Zugriffsrechten ausländischer Behörden, das der Anbieter aufgrund rechtlicher Vorgaben nicht lösen kann: Die Weisungsbindung in Ziff. 3.c.i, ii des „Cisco Master Data Protection Agreement“, Version 1.0 – Germany, 1. Dezember 2020, genügt nicht den Anforderungen von Art. 28 Abs. 3 lit. a DS-GVO, da sie Verarbeitungen außerhalb der Weisungen auch im Fall von Verpflichtungen des Anbieters aus anderem Recht als dem der Europäischen Union oder der Mitgliedstaaten, dem der Anbieter unterliegt, erlaubt. Gleichfalls genügt auch die Pflicht zur Information über entsprechende Verarbeitungen nicht den Anforderungen des Art. 28 Abs. 3 lit. a DS-GVO. Die Standardvertragsklauseln genügen für sich nicht, um Übermittlungen personenbezogener Daten in die USA zu rechtfertigen, da keine ausreichenden ergänzenden Maßnahmen bestehen, um nach europäischem Recht unzulässige Zugriffe von US-Behörden zu verhindern. Für andere Drittländer ohne Angemessenheitsbeschluss der EU-Kommission ist keine Bewertung möglich. Die rechtswidrigen Datenexporte lassen sich nur teilweise vermeiden. Cisco hat angekündigt, Mitte 2021 neue Rechenzentren in der EU in Betrieb zu nehmen und jedenfalls den Mangel unzulässiger Datenexporte im Rahmen der Telemetrie-Funktionen zu beheben. Im Rahmen unserer kursorischen Prüfung mussten wir zudem feststellen, dass standardmäßig weitere, nicht im Vertrag erlaubte Subauftragnehmer eingeschaltet werden. Dies soll nach Angaben von Cisco allerdings deaktivierbar sein.

Aufgrund der rechtlichen Mängel erfolgte keine technische Bewertung.

Cisco Webex Meetings über Telekom

Im „Anhang AVV zum Vertrag über Telekommunikationsleistungen“ mit den Annexen für Cisco Webex – Conferencing und Collaboration Konferenzlösungen (Version 3.0 vom 14.12.2020) an sich haben wir keine Mängel gefunden. Allerdings werden nach dem Vertrag bestimmte, sehr beschränkte Sätze personenbezogener Daten zu Abrechnungszwecken in die USA übermittelt, namentlich Vorname, Name und E-Mail-Adresse der Gastgeberin/des Gastgebers der Videokonferenz und technische Informationen zur Videokonferenz (URL, Start- und Ende-Zeit der Videokonferenz). Im Fall von 24/7-Support können ebenfalls personenbezogene Daten in die USA übermittelt werden.

Für derartige Übermittlungen personenbezogener Daten in die USA fehlt es an einer Rechtsgrundlage. Allerdings ist es möglich, als „Gastgeber“ andere als Realdaten anzugeben, konkret eine Art Gruppen-Account, über den zentral im Unternehmen bzw. in der Behörde die Videokonferenzen organisiert werden. Ist dadurch ein Personenbezug ausgeschlossen, liegt keine Übermittlung personenbezogener Daten in die USA vor, eine Rechtsgrundlage hierfür ist daher nicht erforderlich. Zu beachten ist, dass eine Nutzung der zentralen Zugangsdaten durch verschiedene Personen (statt einer zentralen Stelle) nur dann in Betracht kommt, wenn im Rahmen des administrativen Zugriffs kein Zugang zu personenbezogenen Rahmen- oder Inhaltsdaten anderer Videokonferenzen möglich ist.

Sollte es möglich sein, mit dem Sub-Auftragsverarbeiter Cisco Standardvertragsklauseln abzuschließen, wäre auch denkbar, nicht aufdeckbare persönliche Pseudonyme zur Benennung der Gastgeber zu verwenden. Zu beachten ist in diesem Fall jedoch, dass die Pseudonyme auch nicht durch andere, möglicherweise dem Zugriff der US-Behörden unterliegende Informationen aufdeckbar sein dürfen. Werden die Einladungs-Links also etwa durch die Gastgebenden per E-Mail an Teilnehmende versandt, die US-Dienstleister nutzen, kommt diese Lösung nicht in Betracht, weil US-Behörden die Informationen zusammenfügen und das Pseudonym aufdecken könnten. Eine Lösung mit Pseudonymen erscheint daher im Wesentlichen nur für die interne Kommunikation in größeren Organisationen realisierbar. Im Einzelfall kommt auch die Einholung einer wirksamen Einwilligung in Betracht. Auf die hohen Anforderungen an eine wirksame Einwilligung insbesondere im Beschäftigungs- oder Schul-Kontext weisen wir ausdrücklich hin. Insbesondere müssen die betroffenen Personen die freie Wahl zwischen Einwilligung und Verweigerung der Einwilligung haben, es dürfen ihnen also bei Verweigerung der Einwilligung keine Nachteile entstehen. Darüber hinaus sind die besonderen Anforderungen aus Art. 49 Abs. 1 lit. a DS-GVO zu beachten.

24/7-Support kann mit Datenexporten in unsichere Drittstaaten verbunden sein. Soll dieser genutzt werden, muss daher eine Rechtfertigung hierfür gefunden werden, was äußerst aufwendig und in manchen Konstellationen unmöglich sein dürfte (siehe hierzu die „Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data“ des Europäischen Datenschutzausschusses, abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en). In besonderen Ausnahmefällen mag auch eine Einwilligung denkbar sein, wobei die zusätzlichen Anforderungen aus Art. 49 Abs. 1 lit. a DS-GVO zu beachten sind.

Hinsichtlich des 24/7-Supports kann allerdings mit der Telekom vereinbart werden, dass personenbezogene Daten nur mit ausdrücklicher Zustimmung der Kundinnen und Kunden in die USA übermittelt werden. Die Kundinnen und Kunden können in diesem Fall vorab eine Einwilligung der betroffenen Personen einholen – die vorstehend beschriebenen hohen Anforderungen an eine wirksame Einwilligung sind auch hier zu beachten – oder, falls dies nicht (wirksam) möglich ist, von einer Weiterverfolgung des Falls im 24/7-Support absehen.

Allerdings mussten wir im Rahmen unserer technischen Prüfung feststellen, dass unrechtmäßige Datenexporte erfolgten, die nicht vom Vertrag gedeckt sind. Unmittelbar ersichtlich sind die Datenexporte, die in Verbindung mit der in die verschiedenen Clientprogramme eingebetteten Telemetrie-Funktion stehen, mit der Daten in die USA exportiert werden, die Angaben über die Nutzung des Dienstes durch die Konferenzteilnehmer*innen enthalten. Diese Funktion lässt sich nach Angaben von Cisco auch nicht durch Verantwortliche deaktivieren. Cisco hat eine Behebung dieses Mangels für Mitte 2021 angekündigt.

Weitere Datenexporte in die USA und andere Drittländer sowie die Einschaltung im Vertrag nicht vorgesehener Unterauftragsverarbeiter, die wir im Rahmen unserer kursorischen Prüfung festgestellt hatten und/oder die im Vertrag vorgesehen sind, lassen sich nach Angaben von Cisco und der Telekom durch geeignete Konfiguration und zusätzliche Weisungen durch die Verantwortlichen unterbinden, oder sie lassen sich durch technische, organisatorische und möglicherweise auch durch rechtliche Maßnahmen durch die Verantwortlichen vermeiden oder legalisieren. Da uns Cisco und die Telekom eine datenschutzgerechte Konfiguration in dem zeitlichen Rahmen unserer Prüfung nicht bereitstellen konnten, stellen wir die Bewertung diesbezüglich zurück.

Aufgrund der rechtlichen Mängel erfolgte keine technische Bewertung.

Cloud1X Meet – powered by Jitsi

In der Standardkonfiguration sind die Konferenzen nicht durch Passwort geschützt. Verantwortliche sollten daher vor dem Starttermin und bevor andere Teilnehmende die Konferenz betreten, die Konferenz eröffnen und ein Passwort setzen.

Um eine teilnehmende Person dauerhaft von der Konferenz auszuschließen, ist es der moderierenden Person möglich, ein neues Passwort zu setzen und die Funktion „Hinauswerfen“ auf die Person anzuwenden.

Bei der Transportverschlüsselung haben wir keine Mängel festgestellt. Im Zuge der Authentifizierung von Personen, die die Moderationsrolle übernehmen, wird entsprechend dem Stand der Technik die Übertragung des Passworts an den Anbieter vermieden.

Google Meet (als Teil von Google Workspace unter Geltung des Google Workspace (Online) Agreement und des Data Processing Amendment to Google Workspace and/or Complimentary Product Agreement)

Mängel im Auftragsverarbeitungsvertrag. Unzulässige Einschränkungen des Weisungsrechts. Unzulässige Datenexporte.

Ziff. 6.1 des „Data Processing Amendment to Google Workspace and/or Complimentary Product Agreement, Version 2.3“ (folgend: „DPA“) schränkt das Weisungsrecht hinsichtlich der Datenlöschung und die Benachrichtigungspflicht entgegen Art. 28 Abs. 3 lit. a DS-GVO ein, indem Google sich eine Löschrfrist von 180 Tagen einräumt und zudem die Löschrpflicht unzulässig auch aufgrund von mitgliedstaatlichem Recht ausschließt, dem Google nicht unterliegt. Die Löschrpflicht nach Auftragserledigung nach Art. 28 Abs. 3 lit. g DS-GVO wird durch Ziff. 6.2 DPA unzulässig eingeschränkt, indem Google sich auch insoweit eine Löschrfrist von 180 Tagen einräumt.

Das DPA enthält entgegen Art. 28 Abs. 3 lit. h DS-GVO keine umfassende Verpflichtung für Google, den Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung zu stellen. Ziff. 7.5.1, 7.5.3.a und 7.5.3.b DPA sehen nur ein beschränktes Einsichtsrecht in bestimmte durch Google beauftragte Reports vor.

Ziff. 7.5.3.c DPA sieht eine Vergütungspflicht für jede Art von Überprüfungen durch Verantwortliche vor. Jedenfalls dadurch, dass keine Ausnahmen für durch Vertragsverstöße erforderlich gewordene Überprüfungen gemacht werden, wird durch diese zunächst zivilrechtliche Regelung das Überprüfungsrecht weitgehend entwertet, sodass Art. 28 Abs. 3 lit. h DS-GVO verletzt ist.

Das Verfahren zur Information über gegenwärtige Unterauftragsverarbeiter in Ziff. 11.1 DPA stellt nicht sicher, dass Verantwortliche nachweisen (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) können, welche Unterauftragsverarbeiter mit Vertragsschluss genehmigt wurden. Googles „Affiliates“ sind pauschal als Unterauftragsverarbeiter erlaubt, wobei der Begriff dynamisch definiert ist. Durch gesellschaftsrechtliche Änderungen kann es damit zur Einbeziehung weiterer Unterauftragsverarbeiter kommen, ohne dass Verantwortliche hiergegen ein Widerspruchsrecht haben, wie nach Art. 28 Abs. 2 Satz 1 DS-GVO zwingend erforderlich.

Ziff. 11.3.a.ii DPA stellt nicht sicher, dass – wie von Art. 28 Abs. 4 Satz 1 DS-GVO verlangt – weiteren Auftragsverarbeitern dieselben Datenschutzpflichten auferlegt werden, die im DPA festgelegt sind, sondern beschränkt dies auf Verpflichtungen, die in Art. 28 Abs. 3 DS-GVO beschrieben sind.

Die Beschreibung der Information über neue Unterauftragsverarbeiter in Ziff. 11.4 DPA ist jedenfalls im Zusammenspiel mit Ziff. 11.2 DPA unklar, weil sie auch so ausgelegt werden kann, dass die Information nicht proaktiv erfolgt, sondern nur über eine Website, was nach Art. 28 Abs. 2 Satz 2 DS-GVO nicht genügt. Damit können Verantwortliche zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 11.4(b) DPA gewährt den Verantwortlichen als einzige Widerspruchsmöglichkeit gegen die Einbeziehung neuer Unterauftragsverarbeiter das Recht zur Kündigung des Vertrages. Dieses Recht wird jedoch in der Praxis massiv eingeschränkt, indem Ziff. 8.7 der „Google Workspace Terms of Service, Last modified: December 21, 2020“ (folgend: „ToS“) im Fall einer Kündigung vorsehen, dass keinerlei Erstattung von Entgelten erfolgen. Dies gilt ausdrücklich auch für Kündigungen auf Basis des DPA.

Ziff. 13 DPA beschränkt die Verpflichtungen aus den Standardvertragsklauseln unzulässig, sodass diese nicht zur Rechtfertigung des Datenexports herangezogen werden können. Konkret beschränkt wird die Haftung aus Ziff. 6.2 der Standardvertragsklauseln, weil unter den Begriff der Affiliates in Ziff. 13.1 DPA auch eine natürliche Person fallen kann, die nicht selbst Vertragspartner oder Verantwortlicher ist. Zudem verweist Ziff. 13.2 ergänzend auf Ziff. 13 ToS, die in Ziff. 12.1 und 12.2 jegliche Haftung im Zusammenhang mit dem Nutzungsvertrag einschränken, und zwar nicht beschränkt auf die Parteien. Die salvatorische Klausel in Ziff. 12.3 ToS umfasst – unabhängig von der Frage, ob salvatorische Klauseln für Haftungsausschlüsse überhaupt zulässig sind – nur solche Angelegenheiten, für die eine Haftungsbegrenzung bzw. ein Haftungsausschluss gesetzlich ausgeschlossen sind. Die Haftung nach Ziff. 6.2 der Standardvertragsklauseln stellt aber eine vertragliche Haftungsübernahme dar, die über die gesetzliche Haftung hinausgeht.

Ziff. 1.5(d) ToS erlaubt Google einseitige Änderungen des DPA, die rein durch Veröffentlichung auf der entsprechenden Webseite erfolgen. Dies macht es Verantwortlichen jedenfalls unmöglich, ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) nachzukommen.

Hinweis (nicht notwendig Mangel): Es ist im Einzelfall zu prüfen, ob die in Ziff. 7.1.1 DPA abschließend definierten technisch-organisatorischen Maßnahmen den Anforderungen des Art. 32 DS-GVO genügen. Darüber hinaus enthält das DPA Klauseln, die noch einer genaueren Bewertung bedürfen.

Aufgrund der rechtlichen Mängel erfolgte keine technische Prüfung.

GoToMeeting

Mängel im Auftragsverarbeitungsvertrag. Unzulässig beschränkter Anwendungsbereich. Unzulässige Datenexporte.

Ziff. 5.1 des „Data Processing Addendum, Revised: December 15, 2020“ sieht entgegen Art. 28 Abs. 4 Satz 1 DS-GVO Überprüfungen bei Unterauftragnehmern und vertragliche Vereinbarungen mit diesen nur dann vor, wenn es sich nicht um Konzernunternehmen von LogMeln handelt. Zudem müssen entgegen Art. 28 Abs. 4 Satz 1 DS-GVO die vertraglichen Datenschutz-Verpflichtungen nur „im Wesentlichen“ auch den Unterauftragnehmern auferlegt werden.

Das Verfahren zur Information über gegenwärtige Unterauftragsverarbeiter in Ziff. 5.2 des „Datenverarbeitungsnachtrags“ stellt nicht sicher, dass Verantwortliche nachweisen (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) können, welche Unterauftragsverarbeiter mit Vertragsschluss genehmigt wurden. Das Verfahren zur Information über neue Unterauftragsverarbeiter in Ziff. 5.2 erfordert ein aktives Handeln der Verantwortlichen und genügt damit nicht Art. 28 Abs. 2 Satz 2 DS-GVO. Verantwortliche, die die Benachrichtigungen nicht selbst aktiv abonnieren, können zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 6.2 des „Datenverarbeitungsnachtrags“ genügt nicht den Anforderungen des Art. 28 Abs. 3 lit. h DS-GVO an Nachweispflichten und Kontrollrechte.

Ziff. 10 des „Datenverarbeitungsnachtrags“ beschränkt die Anwendbarkeit bestimmter, in diesem Abschnitt genannter, zwingend erforderlicher Regelungen auf einen Ausschnitt der Verarbeitungen personenbezogener Daten, die der DS-GVO unterliegen; Art. 3 DS-GVO ist viel weiter.

Ziff. 10.3 i. V. m. Anhang 1 des „Datenverarbeitungsnachtrags“ sieht Einschränkungen der Standardvertragsklauseln vor, die zwar wegen einer Vorrangregelung für die Standardvertragsklauseln in Ziff. 12 zivilrechtlich nicht gelten dürften, aber dennoch zu einer unzulässigen Abwandlung führen, sodass diese den Datenexport nicht rechtfertigen können. Die Selbstzertifizierung nach dem Privacy Shield bezieht sich nicht auf HR-Daten.

Aufgrund der rechtlichen Mängel erfolgte keine technische Prüfung.

mailbox.org – Jitsi

Bei der Einrichtung einer neuen Konferenz werden automatisch zwei Passwörter (Teilnahme-passwort und Moderationspasswort) gesetzt, die aber jeweils durch ein eigenes Passwort mit einer Mindestlänge und -komplexität ersetzt werden können.

Um eine teilnehmende Person dauerhaft von der Konferenz auszuschließen, ist es der moderierenden Person möglich, ein neues Passwort zu setzen und die Funktion „Hinauswerfen“ auf die Person anzuwenden.

Bei der Transportverschlüsselung haben wir keine Mängel festgestellt. Das Authentifizierungsverfahren entspricht nicht dem Stand der Technik und überträgt das Passwort innerhalb der TLS-Sitzung an den Dienst.

meetzi – Jitsi

Das Angebot erfüllt die von uns angewandten Prüfkriterien. Das Authentifizierungsverfahren entspricht nicht dem Stand der Technik und überträgt das Passwort innerhalb der TLS-Sitzung an den Dienst.

Microsoft Teams (als Teil von Microsoft 365 unter Gültigkeit der Online Service Terms)

Grundsätzlich bleibt nach den Regelungen im „Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste“ (folgend: „DPA“) diejenige Version des DPA gültig, die bei Abschluss oder Verlängerung des Onlinedienst-Abonnements gültig war. Verantwortliche, die den Dienst bereits abonniert haben, müssen daher prüfen, welche DPA-Version für sie gültig ist.

Dennoch hat Microsoft das DPA „Deutsch, Januar 2020“ ohne Kennzeichnung nachträglich umfangreich geändert. Es gibt ein Dokument, das ausweislich der Metadaten am 3.1.2020 erstellt wurde und ein Dokument, das ausweislich der Metadaten am 9.6.2020 erstellt wurde. Die Bezeichnung der Dokumente ist gleich, das von Microsoft im Internet veröffentlichte Dokument wurde stillschweigend ersetzt. In der Änderungshistorie („Verdeutlichungen und Zusammenfassung der Änderungen“) steht ausdrücklich „Keine“, obwohl große Teile des Vertrags geändert wurden. Microsoft weist insoweit darauf hin, dass es sich bei dem Dokument um eine Übersetzung des englischen Dokuments handle, das selbst nicht geändert worden ist. Es seien dabei nur Korrekturen vorgenommen worden. Letzteres ist jedoch nicht korrekt, sondern es erfolgten nicht nur Anpassungen an die englische Fassung des DPA, sondern teilweise neue, ursprünglich nicht vorhandene Abweichungen der deutschen Fassung von der englischen Fassung.

Wir weisen darauf hin, dass wir angesichts der nachträglichen und nicht dokumentierten Änderung des veröffentlichten Auftragsverarbeitungsvertrags durch Microsoft bei Prüfungen beabsichtigen, auch die Einhaltung der Form des Auftragsverarbeitungsvertrags gemäß Art. 28 Abs. 9 DS-GVO und die entsprechende Nachweisbarkeit (Art. 5 Abs. 2 DS-GVO) zu prüfen.

Microsoft vertritt die Ansicht, dass das DPA in den verschiedenen Fassungen den Vorgaben des anwendbaren Datenschutzrechts entspreche, insbesondere des Art. 28 DS-GVO. Wir können dieser Auffassung aus den im Folgenden genauer dargestellten Gründen nicht folgen.

Aufgrund der rechtlichen Mängel erfolgte keine technische Prüfung.

a) DPA Januar 2020 (in den Versionen vom 3.1.2020 und vom 9.6.2020)

Anbieter behält sich die Verarbeitung von Auftragsdaten zu eigenen Zwecken vor. Mängel im Auftragsverarbeitungsvertrag. Viele Unklarheiten und Widersprüche im Auftragsverarbeitungsvertrag. Unzulässige Datenexporte. Anbieter hat veröffentlichten Auftragsverarbeitungsvertrag ohne Kennzeichnung umfangreich nachträglich geändert; Version (laut Metadaten) vom 3.1.2020 enthält unzulässige Einschränkungen des Weisungsrechts.

Die meisten der stillschweigenden Änderungen zwischen dem DPA Januar 2020 – Version vom 3.1.2020 – und dem DPA Januar 2020 – Version vom 9.6.2020 – sind rein sprachlicher Art. Insbesondere wurde in der Version vom 9.6.2020 die Anlage Standardvertragsklauseln, die ursprünglich sehr umfangreiche Abweichungen vom Wortlaut der genehmigten Standardvertragsklauseln enthielt, im Wesentlichen dem genehmigten Text angepasst. Allerdings gibt es auch relevante inhaltliche Änderungen. Die meisten Änderungen sind positiv zu bewerten. Dennoch bleibt eins der wichtigsten Grundprobleme des Vertrags, dass er an vielen Stellen unklar und widersprüchlich ist, bestehen.

Microsoft behält sich im DPA Januar 2020 unter dem Punkt „Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse“ die Verarbeitung eigentlich im Auftrag verarbeiteter personenbezogener Daten zu eigenen Zwecken vor. Eine Rechtsgrundlage für die damit verbundene Offenlegung personenbezogener Daten durch den Verantwortlichen an Microsoft ist nicht ersichtlich. Aus der Verarbeitung der Auftragsdaten auch zu eigenen Zwecken von Microsoft folgt die Problematik einer gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO. Eine solche liegt nach der Rechtsprechung des EuGH nahe, ist jedenfalls anhand der nur rudimentären Angaben im DPA Januar 2020 nicht auszuschließen. Dies ist mindestens im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) ein Problem. Im Fall des tatsächlichen Vorliegens kommt hinzu, dass keine Vereinbarung nach Art. 26 DS-GVO besteht.

Das DPA Januar 2020 enthält an vielen Stellen Regelungen, die den gesetzlichen Mindestanforderungen widersprechen. Es gibt zwar im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO“ einen in seiner Bedeutung unklaren Verweis auf Anlage 3 zum DPA Januar 2020, die wiederum wesentliche Inhalte aus den Art. 28, 32 und 33 DS-GVO wiedergibt, doch lässt auch die Anlage 3 im Unklaren, ob diese Regeln nun für Microsoft verpflichtend dem eigentlichen – klar rechtswidrigen – Text des DPA Januar 2020 vorgehen sollen oder nicht. Die Datei-Version vom 9.6.2020 verschlechtert diese Klausel sogar noch, indem sie nun von „[den] personenbezogenen Daten der DSGVO“ spricht. Ein derartig unklarer Auftragsverarbeitungsvertrag macht es den Verantwortlichen unmöglich, ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO nachzukommen.

Aber auch Anlage 3 zum DPA Januar 2020 (in der Datei-Fassung vom 3.1.2020) übernimmt den relevanten Wortlaut des Art. 28 DS-GVO nicht vollständig. Jedenfalls Ziff. 2 lit. g der Anlage 3 (in der Datei-Fassung vom 3.1.2020) bleibt hinter den gesetzlichen Mindestanforderungen des Art. 28 Abs. 3 lit. g DS-GVO zurück, indem eine Löschung oder Rückgabe der Auftragsdaten nach Auftragsende nur auf Wunsch der Kundin oder des Kunden vorgesehen ist und nicht in jedem Fall. Ziff. 2 lit. a der Anlage 3 (in der Datei-Fassung vom 3.1.2020) schränkt zudem das Weisungsrecht der Kundinnen und Kunden unzulässig entgegen Art. 28 Abs. 3 lit. a DS-GVO ein, weil Ausnahmen nicht nur aufgrund des Unionsrechts oder des Rechts der Mitgliedstaaten, dem Microsoft unterliegt, vorgesehen sind. In der Datei-Fassung vom 9.6.2020 sind diese Mängel stillschweigend behoben worden, ebenso wie der Wortlaut der Anlage weiter an den Wortlaut des Gesetzes angenähert wurde. Allerdings wurde auch teilweise der Wortlaut des Gesetzes aus der Version vom 3.1.2020 in der Version vom 9.6.2020 durch eigene Begriffe ersetzt. Zudem wurde eine neue Abweichung von den Mindestanforderungen des Art. 28 Abs. 3 lit. a DS-GVO eingefügt, indem die Pflicht zur Benachrichtigung der Kundin oder des Kunden, wenn Microsoft zur weisungswidrigen Datenverarbeitung verpflichtet ist, nicht nur aufgrund des für die Verarbeitungspflicht maßgeblichen Rechts, sondern aufgrund jeden Rechts (Wortlaut „die Gesetzgebung“) ausgeschlossen wird. Eine weitere Abweichung zu Lasten der Kundin oder des Kunden in der Neufassung vom 9.6.2020 von Ziff. 7 der Anlage 3 ist, dass Microsoft die für die Meldung einer sog. Datenpanne erforderlichen Informationen nur noch dann den Kundinnen und Kunden zur Verfügung stellen muss, sofern (statt soweit, also nunmehr nur noch dann, wenn die Bedingung für alle Informationen erfüllt ist und nicht mehr wie vorher teilweise, wenn die Bedingung für Teile der Informationen erfüllt ist) diese Informationen Microsoft nach billigem Ermessen zur Verfügung stehen (statt der objektiven Formulierung

„in angemessener Weise“ also nunmehr auf eine nur beschränkt gerichtlich überprüfbare Billigkeitsentscheidung von Microsoft abstellend).

Im DPA Januar 2020 sind unter dem Punkt „Datensicherheit – Prüfung der Einhaltung“ Einschränkungen der Standardvertragsklauseln vorgesehen. Diese werden als „Zusatz zu Klausel 5, Absatz f und Klausel 12, Absatz 2 der Standardvertragsklauseln“ bezeichnet und es wird behauptet, die Standardvertragsklauseln würden hierdurch nicht abgeändert. Zwar besteht in der Einleitung des DPA Januar 2020 eine allgemeine Aussage, dass die Standardvertragsklauseln dem DPA Januar 2020 vorgehen, wie auch die Standardvertragsklauseln mit ihrem Abänderungsverbot selbst eine entsprechende Vorrangregelung enthalten. Fraglich – und im Hinblick auf Art. 5 Abs. 2 DS-GVO problematisch – ist bereits, ob die allgemeine Vorrangklausel in der Einleitung des DPA Januar 2020 überhaupt anwendbar ist, wenn die in Rede stehende konkrete Einschränkung der Standardvertragsklauseln selbst von sich behauptet, keine Einschränkung darzustellen, sodass unter dieser Annahme die Vorrangklausel denkllogisch nicht zur Anwendung kommen kann. Dies kann allerdings offenbleiben, weil jede Einschränkung der Rechte und Pflichten aus den Standardvertragsklauseln, unabhängig von ihrer Formulierung und auch wenn sie an anderer Stelle für nachrangig und damit nicht anwendbar erklärt wird, zu einer unzulässigen Abwandlung der Standardvertragsklauseln führt. Denn damit wird bezweckt und im Ergebnis regelmäßig auch erreicht, dass die Standardvertragsklauseln nicht vollständig angewendet werden können. Dementsprechend betont auch Erwägungsgrund 109 DS-GVO, dass sonstige Vertragsklauseln weder mittelbar noch unmittelbar im Widerspruch zu den Standard-Datenschutzklauseln stehen dürfen. Somit führt auch die vorliegende Einschränkungs-„Zusatz“-Klausel trotz ihrer mutmaßlichen zivilrechtlichen Unwirksamkeit zu einer unzulässigen Abwandlung der Standardvertragsklauseln, sodass diese den Datenexport nicht rechtfertigen können. Microsoft hat sich zwar zusätzlich einer Selbstzertifizierung nach dem Privacy Shield unterworfen, doch der diesbezügliche Angemessenheitsbeschluss der EU-Kommission wurde durch den EuGH mit Urteil vom 16.7.2020 (Rs. C-311/18 – „Schrems II“) für ungültig erklärt. Microsoft behält sich eine Verarbeitung der Auftragsdaten an jedem Ort vor, an dem Microsoft oder seine Unterauftragsverarbeiter tätig sind (DPA Januar 2020, Abschnitt „Datenschutzbestimmungen – Datenübermittlungen und Speicherstelle – Datenübermittlungen“), also auch in den USA. Zudem ist nicht ersichtlich, dass ausreichende zusätzliche Maßnahmen getroffen worden wären, um entsprechend der Rechtsprechung des EuGH im Urteil „Schrems II“ das unzureichende Datenschutzniveau der USA auszugleichen.

Wir empfehlen, bei einer genaueren Prüfung des DPA Januar 2020 auch die Anmerkungen zum DPA Juli 2020 zu berücksichtigen, die möglicherweise Hinweise auf hier nicht im Detail ausgeführte Probleme geben könnten.

b) DPA Juli 2020, Additional Safeguards Addendum to Standard Contractual Clauses November 2020, DPA Dezember 2020

Unter dem Vorbehalt vorrangiger Sonderregelungen in den „Nutzungsrechten“: Unklarer Umfang der Auftragsverarbeitung. Anbieter behält sich die Verarbeitung von Auftragsdaten zu eigenen Zwecken vor. Mängel im Auftragsverarbeitungsvertrag. Viele Unklarheiten und Widersprüche im Auftragsverarbeitungsvertrag. Unzulässige Datenexporte. Unzulässige Einschränkungen des Weisungsrechts.

Auch das DPA „Letzte Aktualisierung: 21. Juli 2020“ (hier als „DPA Juli 2020“ bezeichnet) nimmt umfangreiche sprachliche Änderungen gegenüber den Vorversionen vor, aber auch einige relevante inhaltliche Änderungen. Eins der wichtigsten Grundprobleme des Vertrags, dass er an vielen Stellen unklar und widersprüchlich ist, bleibt allerdings auch in dieser Version bestehen.

Die Regelungen des DPA Juli 2020 stehen unter dem Vorbehalt, dass Sonderregelungen in „Nutzungsrechten“ enthalten sein können, die dem DPA vorgehen. Wir konnten zwar bei unseren Recherchen keine derartigen vorrangigen Sonderregelungen feststellen, doch ist

nicht auszuschließen, dass solche vorrangigen Sonderregelungen bestehen. Microsoft hat auf unsere diesbezügliche Anfrage leider nicht reagiert, sodass Verantwortliche diesen Aspekt umfassend selbst prüfen müssen.

Microsoft hat Ende November 2020 „Additional Safeguards Addendum to Standard Contractual Clauses“ angekündigt. Deren Inhalt haben wir an relevanter Stelle angesprochen. Das „Microsoft Online Services Data Protection Addendum, Last updated December 9, 2020“ (hier als „DPA Dezember 2020“ bezeichnet) übernimmt im Wesentlichen nur die Regelungen der „Additional Safeguards Addendum to Standard Contractual Clauses“ in das DPA. Es liegt bisher nur in englischer Sprache vor. Soweit bei der Übersetzung ins Deutsche nur die Änderungen vorgenommen werden, die auch in der englischen Sprachfassung erfolgt sind, sind DPA Juli 2020 und DPA Dezember 2020 daher – soweit hier relevant – gleich zu bewerten.

Da das DPA Juli 2020 sehr kompliziert strukturiert ist und an verschiedenen Stellen widersprüchliche Regelungen enthält, erfolgt die Darstellung der gefundenen Mängel und Hinweise im Folgenden im Wesentlichen anhand des Gesetzeswortlauts.

Anwendungsbereich

Es bleibt unklar, in welchem Umfang genau nach dem DPA Juli 2020 eine Auftragsverarbeitung vorliegen soll und in welchem Umfang Microsoft als Verantwortlicher handeln soll. Die Einleitung zum Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO“ stellt für die Anwendbarkeit des Abschnitts und der Anlage 3 (objektiv) darauf ab, ob „Microsoft ein Auftragsverarbeiter oder Unterauftragsverarbeiter der personenbezogenen Daten im Sinne der DSGVO ist“. Im folgenden Absatz dagegen „vereinbaren“ Microsoft und die Kundinnen und Kunden, unter welchen Bedingungen Microsoft (Unter-) Auftragsverarbeiter ist – wobei darauf hinzuweisen ist, dass diese Frage nicht der Dispositionsbefugnis der Parteien unterliegt, sondern aus den Tatsachen und den gesetzlichen Definitionen in Art. 4 Nr. 7 und 8 DS-GVO folgt. Es folgt die Regelung, dass, (nur dann,) „wenn Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt,“ Microsoft weisungsgebunden handelt, was ja nun gerade das Wesenselement der Auftragsverarbeitung darstellt. Insofern ergibt sich indirekt, dass die vertragliche Regelung im DPA, nach der sich Microsoft begrenzt als Auftragsverarbeiter definiert, wegen der aus der Definition als Auftragsverarbeiter vertraglich folgenden begrenzten Weisungsunterwerfung dazu führt, dass Microsoft im Umfang der vertraglichen Definition als Auftragsverarbeiter tatsächlich Auftragsverarbeiter im Sinne des Gesetzes ist. Dies gilt jedenfalls im Ansatz, unter Nichtbeachtung weiterer Einschränkungen der Weisungsbindung im DPA. Es ergibt sich insoweit allerdings das dogmatische Problem, dass nach der Regelung in der Einleitung zum Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO“ die Regelungen, die über die Anwendbarkeit oder Nichtanwendbarkeit der Regelungen zur Rollenfestlegung entscheiden, vom Ergebnis der Rollenfestlegung abhängen.

Das praxisrelevantere Problem ergibt sich daraus, dass die Regelungen zur Rollenfestlegung als (Nicht-) Auftragsverarbeiter im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ auf die „spezifischen Bedingungen des jeweiligen Online-diensts oder in diesem DPA“ verweisen, in denen etwas anderes bestimmt sein kann. Im Falle des DPA Juli 2020 betrifft dies klar die Verarbeitung der personenbezogenen Daten „zu legitimen Geschäftstätigkeiten von Microsoft“, für die sich Microsoft keiner Weisungsbindung unterwirft. Inwieweit andere Datenverarbeitungen im Auftrag der Verantwortlichen oder in eigener Verantwortlichkeit von Microsoft erfolgen, bleibt unklar. Der Abschnitt „Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse“ gibt dazu nichts her, weil die Dienstbereitstellung und die Verarbeitung zu „legitimen Geschäftstätigkeiten von Microsoft“ auf einer Stufe stehend erlaubt werden. Der Abschnitt „Datenschutzbestimmungen – Verarbeitung zur Bereitstellung der Onlinedienste für den Kunden“ defi-

niert nur, was unter „Bereitstellung“ eines Onlinediensts zu verstehen ist und schließt bestimmte Verarbeitungszwecke, die üblicherweise in Verantwortlichkeit von Microsoft erfolgen würden, aus, „es sei denn, eine solche Verwendung oder Verarbeitung erfolgt nach den dokumentierten Anweisungen des Kunden“. Daraus ergibt sich, dass auch diese Klausel sowohl Verarbeitungen in eigener Verantwortlichkeit von Microsoft als auch im Auftrag der Kundin oder des Kunden umfasst. Die (unzureichende, dazu im Folgenden) Festlegung des Zwecks der Verarbeitung im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Verarbeitungsdetails“ hilft mit ihrem Verweis auf „die Bereitstellung des Onlinediensts gemäß dem Volumenlizenzvertrag des Kunden und für die legitimen Geschäftstätigkeiten von Microsoft in Verbindung mit der Bereitstellung der Onlinedienste für den Kunden“ nicht weiter, weil sie offenkundig im Widerspruch zu den sonstigen Regelungen des DPA Juli 2020 steht, wonach jedenfalls die Verarbeitung für die „legitimen Geschäftstätigkeiten von Microsoft“ gerade keine Auftragsverarbeitung darstellen soll, und weil auch diese Festlegung wieder auf den hier soeben diskutierten Abschnitt „Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse“, des DPA Juli 2020 verweist. Die Abgrenzung und somit das Vorliegen einer Auftragsverarbeitung bleibt daher offen.

Das DPA Juli 2020 gilt gemäß Abschnitt „Datenschutzbestimmungen – Umfang“ in wesentlichen Teilen nicht für „Previews“, auch wenn die Verarbeitung personenbezogener Daten in „Previews“ nicht ausgeschlossen ist.

Nähere Beschreibung der Verarbeitung, Art. 28 Abs. 3 UAbs. 1 S. 1 DS-GVO

Gegenstand, Dauer, Art und Zweck der Verarbeitung sind im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Verarbeitungsdetails“, ggf. i. V. m. der Regelung im Abschnitt „Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse“, des DPA Juli 2020 unzureichend geregelt. Die „Anlage 3 – Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union“ verweist in Ziff. 2 auf den „Lizenzvertrag des Kunden“. Verantwortliche müssen daher selbst prüfen, ob in dem von ihnen abgeschlossenen Vertrag Gegenstand, Dauer, Art und Zweck der Verarbeitung hinreichend klar festgelegt sind.

Entsprechendes gilt für die Art der verarbeiteten personenbezogenen Daten und die Kategorien betroffener Personen, wobei hier zusätzlich auf das Verzeichnis von Verarbeitungstätigkeiten verwiesen wird, ohne dass ersichtlich wäre, dass dieses auch selbst zum Vertragsinhalt würde. Auch der Anhang 1 zu den Standardvertragsklauseln enthält keine abschließenden Listen, zumal die als möglich genannten Kategorien betroffener Personen im Hinblick auf Videokonferenz-Dienste unvollständig sind und die Art der Daten sich nur auf „übermittelte“ personenbezogene Daten beschränkt.

Weisungsbindung und Pflicht zur Mitteilung von Verarbeitungen ohne Weisung, Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a DS-GVO

Zwar enthält die „Anlage 3 – Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union“ unter Ziff. 2.(a) eine Regelung, die für sich genommen den Anforderungen des Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a DS-GVO genügt, doch wird diese Regelung an vielen Stellen des DPA Juli 2020 wieder eingeschränkt, ohne dass erkennbar wäre, dass die allgemeine Klausel in Anlage 3 den detaillierten Regelungen an anderer Stelle des DPA Juli 2020 vorgehen würde. Die Einleitung des Abschnitts „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO“ des DPA Juli 2020 kann zwar möglicherweise – was bereits für sich genommen ein Problem im Hinblick auf die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO darstellt – so verstanden werden, dass dieser Abschnitt anderen Abschnitten des DPA vorgehen soll. Allerdings gilt dies nicht für die Anlage 3 im Verhältnis zu den Regelungen des Abschnitts „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO“, die ausdrücklich „zudem“, also gleichrangig, gelten sollen. Die Regelungen im Unterabschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Auftragsverarbeiter und Verantwortlicher – Rollen und

Verantwortlichkeiten“ enthalten einerseits selbst Einschränkungen des Weisungsrechts, indem der „Volumenlizenzvertrag (einschließlich der DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit der Produktdokumentation und der Verwendung und Konfiguration der Features der Onlinedienste durch die Kundinnen und Kunden die vollständigen und dokumentierten Anweisungen der Kundinnen und Kunden gegenüber Microsoft in Bezug auf die Verarbeitung personenbezogener Daten darstellen“ und im Übrigen auf das Verfahren zur Änderung des Volumenlizenzvertrags verwiesen wird. Andererseits verweist der Unterabschnitt für Ausnahmen von der Rollenverteilung als Auftragsverarbeiter und damit die Weisungsbindung auf die spezifischen Bestimmungen des jeweiligen Onlinediensts und das DPA Juli 2020, somit auch auf die Regelungen etwa unter dem Punkt „Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse“, wo sich Microsoft die Verarbeitung eigentlich im Auftrag verarbeiteter personenbezogener Daten zu eigenen Zwecken vorbehält, unter dem Punkt „Datenschutzbestimmungen – Offenlegung verarbeiteter Daten“, in denen Microsoft sich Offenlegungen der im Auftrag verarbeiteten Daten allgemein auf Basis gesetzlicher Verpflichtungen vorbehält, ohne dass dabei die Anforderungen des Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a DS-GVO eingehalten würden (nur Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt), oder unter dem Punkt „Datenschutzbestimmungen – Speicherung und Löschung von Daten“, wo Microsoft sich ein Unterlassen der Löschung beispielsweise auch dann vorbehält, wenn Microsoft durch beliebiges anwendbares Recht zur Aufbewahrung verpflichtet oder auch nur berechtigt ist.

Auch die „Additional Safeguards Addendum to Standard Contractual Clauses“ (die als „Appendix 3 to the Standard Contractual Clauses – Additional Safeguards Addendum“ in das DPA Dezember 2020 aufgenommen wurden) sehen keine den Anforderungen des Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a DS-GVO entsprechende Verpflichtung vor, sondern setzen im Gegenteil implizit voraus, dass Microsoft die im Auftrag verarbeiteten Daten ohne oder entgegen den Weisungen verarbeitet, weil sie im Kontext von Datenexporten in Drittländer die Verpflichtung von Microsoft vorsehen, die Kundinnen und Kunden unverzüglich über eine erzwungene Offenlegung an Dritte zu benachrichtigen, es sei denn, dies ist nach dem auf den anfragenden Dritten anwendbaren Recht verboten.

Die Verarbeitung eigentlich im Auftrag verarbeiteter personenbezogener Daten zu eigenen Zwecken durch Microsoft, wie Microsoft sie sich vorbehält, bedingt eine Offenlegung personenbezogener Daten durch den Verantwortlichen an Microsoft im rechtlichen Sinne. Eine Rechtsgrundlage für diese Offenlegung ist nicht ersichtlich. Aus der Verarbeitung der Auftragsdaten auch zu eigenen Zwecken von Microsoft folgt die Problematik einer gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO. Eine solche liegt nach der Rechtsprechung des EuGH nahe, ist jedenfalls anhand der nur rudimentären Angaben im DPA Juli 2020 nicht auszuschließen. Dies ist mindestens im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) ein Problem. Im Fall des tatsächlichen Vorliegens kommt hinzu, dass keine Vereinbarung nach Art. 26 DS-GVO besteht.

Auch die Verpflichtung, Verarbeitungen ohne Weisung vor der Verarbeitung mitzuteilen, ist zwar in Anlage 3 Ziff. 2.(a) dem Wortlaut des Gesetzes entsprechend abgebildet, wird aber unter dem Punkt „Datenschutzbestimmungen – Offenlegung verarbeiteter Daten“ unzulässig eingeschränkt, indem einerseits die Verbote auch aus nach Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a DS-GVO unzulässigem Recht (nicht nur Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt) herrühren können und andererseits die Mitteilung nicht (nur) wegen eines wichtigen öffentlichen Interesses verboten sein muss.

Vertraulichkeitsverpflichtung, Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b DS-GVO

Die Regelungen unter dem Punkt „Datenschutzbestimmungen – Vertraulichkeitsverpflichtung des Auftragsverarbeiters“ des DPA Juli 2020 können im Zusammenhang mit den unzulässigen Einschränkungen des Weisungsrechts wohl nur so verstanden werden, dass die Verpflichtung zur Verarbeitung der personenbezogenen Daten befugten Personen zu

Vertraulichkeit in gleichem Maße beschränkt werden soll, was den Anforderungen von Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b DS-GVO nicht entspricht.

Löschpflicht nach Auftrags erledigung, Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g DS-GVO

Hinsichtlich der Pflicht zur Löschung der im Auftrag verarbeiteten Daten nach Auftrags erledigung genügt bereits Ziff. 2.(g) der Anlage 3 zum DPA Juli 2020 nicht den Anforderungen des Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g DS-GVO. An dieser Stelle wird zwar weitestgehend der Gesetzestext übernommen, Kopien sind aber anders als im Gesetzestext nicht genannt. Darüber hinaus enthält der Abschnitt „Datenschutzbestimmungen – Speicherung und Löschung von Daten“ des DPA Juli 2020 diverse Einschränkungen der Löscho- bzw. Rückgabepflicht entgegen Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g DS-GVO, darunter eine lange Umsetzungsfrist für die Löschung und Ausnahmen von der Löschpflicht, wenn Microsoft aus (beliebigem) anwendbarem Recht zur Aufbewahrung verpflichtet oder auch nur berechtigt ist (und somit nicht nur, wenn nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht).

Hinsichtlich der Regelungen im Abschnitt „Datenschutzbestimmungen – Speicherung und Löschung von Daten“ des DPA Juli 2020 ließe sich zwar argumentieren, dass die (für sich ebenfalls nicht rechtskonforme) Anlage 3 insoweit vorrangig gelten solle, wenn man die Einbeziehungsklausel im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO“ als Vorrangklausel interpretiert. Allerdings ergibt sich dies nicht aus dem Wortlaut und würde zudem bedeuten, dass eine sehr allgemein gehaltene Klausel sehr spezifische Regelungen verdrängen würde. In jedem Fall können Verantwortliche beim Vorliegen derart unklarer Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO nicht nachkommen.

Nachweispflichten und Kontrollrechte, Art. 28 Abs. 3 UAbs. 1 lit. h DS-GVO

Ziff. 2.(h) der Anlage 3 zu DPA Juli 2020 enthält für sich genommen eine ausreichende Verpflichtung zum Nachweis der Pflichten aus Art. 28 DS-GVO. Das Verhältnis zum Abschnitt „Datenschutzbestimmungen – Datensicherheit – Prüfung der Einhaltung“ und insbesondere der dort enthaltenen Vertraulichkeitsverpflichtung ist aber unklar. Daraus und aus der unklaren Reichweite dieser Vertraulichkeitsverpflichtung könnte sich das Problem ergeben, dass Verantwortliche ihren Nachweispflichten gegenüber uns als Aufsichtsbehörde oder gegenüber betroffenen Personen etwa im Rahmen der Abwehr von Schadensersatzansprüchen nicht nachkommen können.

Auch hinsichtlich der Kontrollrechte der Verantwortlichen ist Ziff. 2.(h) der Anlage 3 zum DPA Juli 2020 für sich genommen ausreichend. Allerdings enthält insoweit der Abschnitt „Datenschutzbestimmungen – Datensicherheit – Prüfung der Einhaltung“ weiterhin schwerwiegende Einschränkungen der Kontrollrechte der Verantwortlichen. So besteht jedes Prüferecht überhaupt nur, wenn bestimmte von Microsoft bereitgestellte Unterlagen nicht genügen. In diesem Fall muss Microsoft aber auch nur „umgehend auf die zusätzlichen Prüfanweisungen“ der Kundin oder des Kunden „reagier[en]“, nicht aber tatsächlich eine Kontrolle ermöglichen und zu ihr beitragen, wie es Art. 28 Abs. 3 UAbs. 1 lit. h DS-GVO verlangt. Jede Prüfung steht zudem unter dem Vorbehalt, dass sich Microsoft und Kundin/Kunde zuvor über „Umfang, Zeitpunkt, Dauer, Kontroll- und Nachweisanforderungen sowie die Gebühren für die Prüfung“ geeinigt haben; ausgeschlossen wird nur die Berechtigung von Microsoft, „die Durchführung der Prüfung unangemessen zu verzögern“. Die Kundin oder der Kunde muss also auch dann Kosten tragen, wenn die Kontrolle ausschließlich durch Verschulden von Microsoft erforderlich wurde, was das Kontrollrecht datenschutzrechtlich unzulässig entwertet. Die nach Art. 28 Abs. 3 UAbs. 1 S. 2 lit. h DS-GVO zwingend erforderliche Verpflichtung zur Ermöglichung der und zum aktiven Beitragen zu Kontrollen ist nur auf bestimmte Handlungen beschränkt. Kontrollen dürfen nur durch bestimmte Dritte durchgeführt werden, nicht aber durch die Kundin oder den Kunden selbst. Das DPA Juli 2020 sieht zudem eine „angemessene Vorankündigung“ vor, ohne klarzustellen, dass in

besonderen Ausnahmefällen auch eine Kontrolle ohne vorherige Anmeldung angemessen sein kann.

Einschaltung von Subunternehmern, Art. 28 Abs. 2, 4 DS-GVO

Die Regelungen zur Einbeziehung von Unterauftragsverarbeitern durch Microsoft sind in verschiedenen Punkten unklar und widersprüchlich und widersprechen den gesetzlichen Mindestanforderungen.

Im Abschnitt „Datenschutzbestimmungen – Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ im DPA Juli 2020 heißt es zunächst: „Microsoft kann Unterauftragsverarbeiter beauftragen, bestimmte eingeschränkte oder unterstützende Dienstleistungen für Microsoft zu erbringen. Der Kunde erklärt sich einverstanden, dass eine solche Beauftragung erfolgt und dass Microsoft-Gesellschaften als Unterauftragsverarbeiter eingesetzt werden.“ Diese Klauseln erwecken den Eindruck, dass die Kundinnen und Kunden alle „Microsoft-Gesellschaften“ als Unterauftragsverarbeiter genehmigen, also nur der zweite Satz tatsächlich eine (beschränkte) allgemeine schriftliche Genehmigung im Sinne des Art. 28 Abs. 2 S. 1 DS-GVO darstellt. Allerdings spricht der nächste Satz im Plural von den „oben genannten Autorisierungen“, sodass unklar ist, ob nur „Microsoft-Gesellschaften“ als Unterauftragsverarbeiter genehmigt werden oder auch sonstige Dritte. Wer tatsächlich als Unterauftragsverarbeiter konkret wofür eingesetzt werden darf, ergibt sich nicht aus dem DPA Juli 2020, sodass der zweite Satz – vorbehaltlich sonstiger vertraglicher Vereinbarungen – auch nicht eine konkrete Genehmigung der ggf. anderswo definierten und in ihrem Aufgabenbereich beschriebenen „Microsoft-Gesellschaften“ darstellen kann. Das DPA Juli 2020 enthält eine pauschale Aussage, dass Microsoft „Informationen über Unterauftragsverarbeiter auf einer Microsoft-Website zur Verfügung“ stellt. Verantwortliche müssen daher prüfen, ob in ihrem Vertrag im Übrigen konkret benannt ist, welcher (konkret benannte) Unterauftragsverarbeiter für welche (konkret benannte) Tätigkeit eingeschaltet werden darf, um ihren Verpflichtungen aus Art. 5 Abs. 2 DS-GVO nachkommen zu können. Ein pauschaler Verweis auf eine (sich ggf. ändernde) Website, auf dynamisch definierte (und damit bei Änderungen in der Konzernstruktur plötzlich ohne Weiteres andere Gesellschaften umfassende) oder nicht abschließend und präzise aufgeführte Konzerngesellschaften genügt nicht.

Ob neue Unterauftragsverarbeiter nur mit Zustimmung der Verantwortlichen eingeschaltet werden dürfen oder ob eine Widerspruchslösung eingreifen soll, ist nicht ganz klar. Nach dem Wortlaut des Abschnitts „Datenschutzbestimmungen – Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ im DPA Juli 2020 ist eine konkrete Zustimmung im Einzelfall erforderlich („Wenn der Kunde einem neuen Unterauftragsverarbeiter nicht zustimmt...“), wenn nicht die im vorigen Absatz diskutierten Klauseln eine konkrete Zustimmung im Einzelfall zu (dann anderweitig im Vertrag konkret und abschließend mit ihren jeweiligen Aufgabengebieten zu beschreibenden) Unterauftragsverarbeitern im Microsoft-Konzern darstellen sollen. Jedoch regelt Anlage 3 Ziff. 1 des DPA Juli 2020, dass Microsoft „im Fall einer allgemeinen schriftlichen Genehmigung [...] den Kunden immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informieren [wird], wodurch der Kunde die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben“. Als logische Folge einer Einspruchslösung sieht das DPA Juli 2020 für den Fall einer fehlenden Zustimmung nicht etwa ein Kündigungsrecht für Microsoft vor, sondern ausschließlich ein Kündigungsrecht für den Kunden. Natürlich könnte dies einfach eine kundenfreundliche Regelung sein. Es erscheint allerdings kaum denkbar, dass Microsoft im Massengeschäft den Widerspruch eines einzigen Kunden ausreichen lassen wird, um auf die Einschaltung eines Unterauftragsverarbeiters zu verzichten oder jedenfalls für diesen einen Kunden eine gesonderte Technologie ohne Einbeziehung dieses konkreten Unterauftragsverarbeiters zu erstellen. Entsprechend spricht auch eine Stellungnahme von Microsoft uns gegenüber die Möglichkeit zur Kündigung durch den Kunden unter der Überschrift „Widerspruch gegen neue Unterauftragsverarbeiter“ an.

Irgendwelche genaueren Regelungen zum Einspruch gegen neue Unterauftragsverarbeiter fehlen allerdings. Geregelt ist nur die Ankündigungsfrist für neue Unterauftragsverarbeiter im Abschnitt „Datenschutzbestimmungen – Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ im DPA Juli 2020.

Insbesondere im Hinblick auf die Einbeziehung von Unterauftragsverarbeitern, aber auch in anderen Zusammenhängen, etwa bei der Information über Verletzungen des Schutzes personenbezogener Daten, erweist sich die Klausel unter „Einleitung – Elektronische Benachrichtigungen“ des DPA Juli 2020 als problematisch, wonach Microsoft „Informationen und Mitteilungen über Onlinedienste elektronisch, auch per E-Mail, über das Portal des Onlinedienstes oder über eine von Microsoft zu benennende Website zur Verfügung stellen“ kann und solche Benachrichtigungen sogar „an dem Datum als erteilt [gelten], an dem diese von Microsoft zur Verfügung gestellt wurde[n]“. Ein derartiges „Pull“-System, in dem Verantwortliche sich über neue Unterauftragsverarbeiter, Verletzungen des Schutzes personenbezogener Daten o. Ä. selbst aktiv informieren müssen und nicht durch den Auftragsverarbeiter aktiv informiert werden, entspricht nicht den gesetzlichen Anforderungen.

Sollte Microsoft auch ohne Zustimmung im Einzelfall neue Unterauftragsverarbeiter einsetzen wollen, erweist sich der letzte Satz im Abschnitt „Datenschutzbestimmungen – Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ im DPA Juli 2020 als möglicherweise massive Einschränkung des Kündigungsrechts, indem im Fall einer Kündigung nämlich die Zahlungsverpflichtungen für die gekündigten Onlinedienst-Abonnements erst mit der nächsten Rechnung entfallen.

Nach Art. 28 Abs. 4 S. 1 DS-GVO müssen Unterauftragsverarbeitern mittels eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt werden, die zwischen dem Verantwortlichen und dem Auftragsverarbeiter vereinbart sind. Im Abschnitt „Datenschutzbestimmungen – Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ im DPA Juli 2020 ist ein schriftlicher Vertrag nur für die Einhaltung der Zweckbindung durch den Unterauftragsverarbeiter vorgesehen. Nicht näher definierte „schriftliche Vereinbarungen“, die nicht notwendig Rechtsinstrumente nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats sein müssen, müssen danach von den Unterauftragsverarbeitern verlangen, dass sie „mindestens das Datenschutzniveau bieten“, das das DPA Juli 2020 von Microsoft verlangt. Das Gesetz stellt bereits nicht nur auf das Niveau des Datenschutzes ab, sondern verlangt eine Weitergabe derselben Datenschutzpflichten, d. h. es müssen ausnahmslos alle vertraglichen Pflichten des Auftragsverarbeiters auch dem Unterauftragsverarbeiter auferlegt werden. Der Abschnitt des DPA Juli 2020 regelt ausweislich seiner Überschrift auch die „Kontrollen beim Einsatz von Unterauftragsverarbeitern“ dergestalt, dass Microsoft sich verpflichtet, „die Unterauftragsverarbeiter zu beaufsichtigen, um sicherzustellen, dass diese vertraglichen Verpflichtungen erfüllt werden“. Gesetzeskonforme Kontrollrechte für Verantwortliche sieht der Abschnitt nicht vor, aber auch nicht einmal eine Auferlegung der – unzureichenden, siehe oben – Kontrollrechte wie gegenüber Microsoft. Gleiches gilt für die Nachweispflichten. Sollte Anlage 3 dem zitierten Abschnitt vorgehen – was nicht klar ist, sodass in jedem Fall ein Problem im Hinblick auf Art. 5 Abs. 2 DS-GVO besteht –, würde auch die dortige Regelung nicht genügen. Denn auch nach dieser Regelung werden dem Unterauftragsverarbeiter nicht sämtliche vertraglichen Datenschutzpflichten auferlegt, sondern nur „dieselben Datenschutzpflichten [...], die in diesen DSGVO-Bestimmungen beschrieben sind“, also nur die unmittelbar in Anlage 3 aufgeführten Pflichten.

Datenexporte, Art. 44 DS-GVO

Im DPA Juli 2020 sind unter dem Punkt „Datensicherheit – Prüfung der Einhaltung“ Einschränkungen der Standardvertragsklauseln vorgesehen. Diese sollen „zusätzlich zu Klausel 5, Absatz f und Klausel 12, Absatz 2 der Standardvertragsklauseln“ gelten und es wird behauptet, die Standardvertragsklauseln würden hierdurch nicht abgeändert. Zwar besteht

in der Einleitung des DPA Juli 2020 eine allgemeine Aussage, dass die Standardvertragsklauseln dem DPA Juli 2020 vorgehen, wie auch die Standardvertragsklauseln mit ihrem Abänderungsverbot selbst eine entsprechende Vorrangregelung enthalten. Fraglich – und im Hinblick auf Art. 5 Abs. 2 DS-GVO problematisch – ist bereits, ob die allgemeine Vorrangklausel in der Einleitung des DPA Juli 2020 überhaupt anwendbar ist, wenn die in Rede stehende konkrete Einschränkung der Standardvertragsklauseln selbst von sich behauptet, keine Einschränkung darzustellen, sodass unter dieser Annahme die Vorrangklausel denklogisch nicht zur Anwendung kommen kann. Dies kann allerdings offenbleiben, weil jede Einschränkung der Rechte und Pflichten aus den Standardvertragsklauseln, unabhängig von ihrer Formulierung und auch wenn sie an anderer Stelle für nachrangig und damit nicht anwendbar erklärt wird, zu einer unzulässigen Abwandlung der Standardvertragsklauseln führt. Denn damit wird bezweckt und im Ergebnis regelmäßig auch erreicht, dass die Standardvertragsklauseln nicht vollständig angewendet werden können. Dementsprechend betont auch Erwägungsgrund 109 DS-GVO, dass sonstige Vertragsklauseln weder mittelbar noch unmittelbar im Widerspruch zu den Standard-Datenschutzklauseln stehen dürfen. Somit führt auch die vorliegende Einschränkungs-„zusätzlich“-Klausel trotz ihrer mutmaßlichen zivilrechtlichen Unwirksamkeit zu einer unzulässigen Abwandlung der Standardvertragsklauseln, sodass diese den Datenexport nicht rechtfertigen können.

Microsoft behält sich eine Verarbeitung der Auftragsdaten an jedem Ort vor, an dem Microsoft oder seine Unterauftragsverarbeiter tätig sind (DPA Juli 2020, Abschnitt „Datenschutzbestimmungen – Datenübermittlungen und Speicherstelle – Datenübermittlungen“), also auch in den USA. Es ist nicht ersichtlich, dass ausreichende zusätzliche Maßnahmen getroffen worden wären, um entsprechend der Rechtsprechung des EuGH im Urteil vom 16.7.2020 – C-311/18 („Schrems II“) das unzureichende Datenschutzniveau der USA auszugleichen. Auch die „Additional Safeguards Addendum to Standard Contractual Clauses“ (die als „Appendix 3 to the Standard Contractual Clauses – Additional Safeguards Addendum“ in das DPA Dezember 2020 aufgenommen wurden) genügen hierfür ersichtlich nicht, da sie insbesondere weder den Zugriff von US-Behörden auf die verarbeiteten Daten ausschließen noch betroffenen Personen eine Rechtsschutzmöglichkeit gegen Zugriffe durch US-Behörden gewähren.

NETWAYS Web Services Jitsi

Bei dem Angebot von Netways erhält man Moderator-Zugriff auf eine vorkonfigurierte Instanz von Jitsi Meet. Das vorkonfigurierte Moderationspasswort ist lang, kann aber nicht selbst verändert werden. In der Standardkonfiguration sind die Konferenzen nicht durch Passwort geschützt und die Teilnehmenden betreten die Konferenz mit aktiver Kamera und aktivem Mikrofon.

Verantwortliche sollten daher vor dem Starttermin und bevor andere Teilnehmende die Konferenz betreten die Konferenz eröffnen und ein Passwort setzen. Zudem sollten sie für die verwendeten Konferenzräume konfigurieren, dass Teilnehmende mit deaktiviertem Mikrofon und deaktivierter Kamera die Konferenz betreten.

Um eine teilnehmende Person dauerhaft von der Konferenz auszuschließen, ist es der moderierenden Person möglich, ein neues Passwort zu setzen und die Funktion „Hinauswerfen“ auf die Person anzuwenden.

Bei der Transportverschlüsselung haben wir keine Mängel festgestellt. Im Zuge der Authentifizierung von Personen, die die Moderationsrolle übernehmen, wird entsprechend dem Stand der Technik die Übertragung des Passworts an den Anbieter vermieden.

Open Source Company – BigBlueButton

Bei dem von der Open Source Company (OSC) bereitgestellten Angebot erhalten Verantwortliche einen Zugang mit Moderationsrechten auf einer BigBlueButton-Instanz.

Teilnehmende benötigen zum Betreten der Videokonferenz in den Voreinstellungen nur die Adresse (URL) der Konferenz und betreten diese mit aktiviertem Mikrofon und deaktivierter Kamera. Verantwortliche sollten daher für die verwendeten Konferenzräume konfigurieren, dass eine Teilnahme nur für angemeldete Teilnehmende und Gäste mit Kenntnis eines zusätzlichen Zugangscodes möglich ist und dass Teilnehmende mit deaktiviertem Mikrofon die Konferenz betreten. Zusätzlich ist es möglich und ratsam einzustellen, dass eine Freigabe durch die moderierende Person erfolgen muss.

In den Voreinstellungen wird die Videokonferenz erst gestartet, nachdem die moderierende Person sie eröffnet hat. Es ist aber möglich, auch anderen authentifizierten Teilnehmenden die Eröffnung zu erlauben oder Moderationsrechte zu gewähren.

Wir haben keine Mängel bei der Transportverschlüsselung gefunden.

sichere-videokonferenz.de – Jitsi

Eine feste Moderationsrolle gibt es nicht. Moderator*in einer Konferenz wird automatisch die erste Person, die den Konferenzraum betritt. Verlässt sie – und sei es aufgrund von Verbindungsproblemen – den Konferenzraum, geht die Moderationsrolle automatisch auf die Person über, die bereits am längsten an der Konferenz teilnimmt. In den Anwendungsfällen 2 und 3 stellt dies einen Mangel dar.

Bei der Transportverschlüsselung haben wir keine Mängel festgestellt. Das Authentifizierungsverfahren entspricht nicht dem Stand der Technik und überträgt das Passwort innerhalb der TLS-Sitzung an den Dienst.

TeamViewer Meeting (früher Blizz)

Anbieter behält sich die Verarbeitung von Auftragsdaten zu eigenen Zwecken vor. Mängel im Auftragsverarbeitungsvertrag.

Der „TeamViewer Auftragsverarbeitungsvertrag (AVV), Versionsstand 1. Januar 2021“ (folgend: „AVV“) sieht in Ziff. 2.2 nur ein beschränktes Weisungsrecht für Verantwortliche vor.

Ziff. 2.9 Satz 3 AVV gestattet Überprüfungen und Inspektionen nur dann, wenn objektiv begründete Anhaltspunkte für einen Verstoß durch den Anbieter gegen den AVV oder datenschutzrechtliche Regelungen bestehen, und beschränkt die nach Art. 28 Abs. 3 lit. h DSGVO zulässige Einschaltung Dritter als Prüfer auf nicht näher definierte „qualifizierte“ Prüfer.

Ziff. 2.5 und 2.6 AVV sehen vor, dass die Unterstützung durch den Anbieter bei der Wahrung der Betroffenenrechte und der Einhaltung der Art. 32 bis 36 DSGVO kostenpflichtig ist, „sofern und soweit nach anwendbarem Datenschutzrecht zulässig“. Es ist unklar, ob davon auch Fälle erfasst werden sollen, in denen die Unterstützung nur wegen eines Vertrags- oder Gesetzesverstößes des Anbieters erforderlich werden, denn eine solche Vereinbarung ist grundsätzlich zulässig, entwertet jedoch die Verpflichtung umfassend, was wiederum datenschutzrechtliche Folgeprobleme verursacht. Dies ist jedenfalls im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) problematisch.

Ziff. 2.13 AVV enthält am Ende dem Wortlaut nach eine nur durch die Anforderung, Art. 44 ff. DSGVO einzuhalten, beschränkte Erlaubnis für den Anbieter, Unterauftragsverarbeiter in Drittstaaten einzuschalten. Ziff. 3.1 AVV regelt nicht ausdrücklich, dass der Anbieter Unterauftragsverarbeiter nur mit Genehmigung einsetzt. Beides ist im jedenfalls im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) problematisch.

Der AVV verpflichtet den Anbieter nicht ausreichend im Sinne von Art. 28 Abs. 4 Satz 1 DSGVO, Unterauftragsverarbeitern dieselben Datenschutzpflichten aufzuerlegen wie sie für den Anbieter bestehen (vgl. Ziff. 3.3 AVV).

Der AVV enthält in Ziff. 2.2 und Ziff. 3.2 Verweise auf die „TeamViewer Endbenutzer-Lizenzvereinbarung, Versionsstand: 1. Januar 2021“ (folgend: „EULA“), bei denen insbesondere

nicht klar ist, ob dadurch das Weisungsrecht beschränkt werden soll. Dies ist jedenfalls im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) problematisch.

Der Anbieter behält sich in Ziff. 4 AVV ein (inhaltlich nicht näher beschränktes) Recht zur Änderung des AVV vor. Dieses erfüllt nicht einmal die Anforderungen des § 308 Nr. 5 BGB, der nach der Rechtsprechung des BGH über § 307 BGB auch im unternehmerischen Verkehr anwendbar ist (Urteil vom 10. Juni 2008 – XI ZR 283/07; vgl. auch Versäumnisurteil vom 10. September 2014 – XII ZR 56/11), ist darüber hinaus aber auch insoweit problematisch, als dass dadurch dem Anbieter die Möglichkeit gegeben wird, einen rechtswidrigen Vertrag zu erreichen und sogar Zweck und Mittel der Verarbeitung festzulegen.

Nicht Gegenstand der Verarbeitung im Auftrag sind gemäß Ziff. 3 Anlage 1 zu AVV diverse Verarbeitungen personenbezogener Daten durch den Anbieter, wie in der jeweiligen Produktdatenschutzrichtlinie beschrieben. Hierzu gehören nach Ziff. 1.B (gemeint: Ziff. 1.C, die Zwischenüberschrift fehlt) der „TeamViewer Produkt-Datenschutzrichtlinie“ (ohne Versionsnummer, Abruf 4. Februar 2021) (folgend: „PDSRL“) diverse Informationen über Endgeräte, Nutzung, Verbindungspartner usw., unter anderem auch zu Zwecken der Produktverbesserung und der Direktwerbung (vgl. Ziff. 1.D PDSRL). Eine Rechtsgrundlage für die damit verbundene Offenlegung personenbezogener Daten durch Verantwortliche ist nicht ersichtlich. Aus der Verarbeitung der Auftragsdaten auch zu eigenen Zwecken des Anbieters folgt zudem die Problematik einer gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO. Eine solche liegt nach der Rechtsprechung des EuGH nahe, ist jedenfalls anhand der Angaben in der EULA nicht auszuschließen. Dies ist mindestens im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) ein Problem. Im Fall des tatsächlichen Vorliegens kommt hinzu, dass keine Vereinbarung nach Art. 26 DS-GVO besteht.

Aufgrund der rechtlichen Mängel erfolgte keine technische Prüfung.

Tixeo Cloud

Für die Nutzung des Angebots von Tixeo ist zwingend eine Registrierung erforderlich. Da für die Registrierung die Nutzung einer E-Mail-Adresse erforderlich ist, bietet Tixeo gegenüber z. B. Jitsi eine etwas höhere Sicherheit hinsichtlich der Identität der Teilnehmenden. Hinzu kommt, dass einem geplanten Meeting nur eingeladene Teilnehmende beitreten können, was den Verantwortlichen eine Kontrolle über den Kreis der Teilnehmenden ermöglicht.

Tixeo Cloud erfordert die Installation eines Clients auf dem Gerät, auf dem es verwendet werden soll. Eine Nutzung über eine Webseite ist bei diesem Angebot nicht vorgesehen. Es muss also berücksichtigt werden, ob eine Installation von Software in der intendierten Umgebung möglich ist.

Teilnehmende betreten die Konferenz mit aktivierten Eingabegeräten (Mikrofon und Kamera). Dies kann derzeit nicht konfiguriert werden. In den oben beschriebenen Anwendungsfällen stellt dies einen Mangel dar. Der Anbieter hat eine Behebung dieses Mangels für Version 16.5 (geplant für Mitte Februar 2021) angekündigt.

Der Veranstalter eines Meetings hat die Möglichkeit, den Teilnehmenden die Rechte für die Nutzung von Kamera und Mikrofon zu gewähren und zu entziehen. Die Funktion entspricht dabei der Kamera- und Mute-Funktion der jeweiligen Teilnehmenden. Werden die Rechte einer teilnehmenden Person wieder erteilt, wird sie in den Zustand versetzt, den sie vor dem Entzug der Rechte hatte. Dies sollte den Teilnehmenden mitgeteilt werden, da, sobald die Rechte entzogen sind, die jeweiligen Buttons verschwinden und somit die/der Moderator*in die Eingabegeräte einschalten kann, wenn sie vor dem Rechteentzug eingeschaltet waren. Soll diese Funktion genutzt werden, sollten die Teilnehmenden vor Entzug der Rechte darauf hingewiesen werden, dass sie selbst ihre Kamera bzw. ihr Mikrofon deaktivieren sollten, sodass sie auch nach Erteilung der Rechte selbst bestimmen können, wann die Eingabegeräte wieder aktiviert werden.

Zum Zeitpunkt unserer Prüfung haben wir festgestellt, dass die bereitgestellte Tixeo-App kein Certificate Pinning einsetzt. Es besteht dadurch ein erhöhtes Risiko, dass beispielweise

Man-in-the-middle-Angriffe zwischen dem Server und dem Client erfolgreich sind und damit die Integrität und Vertraulichkeit der Kommunikation verletzt wird. Zumindest bei einigen Clients kann und sollte der Verantwortliche ein Certificate Pinning vornehmen. Tixeo stellt hierfür eine Anleitung bereit.

Tixeo bietet eine schwache Variante der Ende-zu-Ende-Verschlüsselung an.

Tixeo hat uns gegenüber angegeben, als Dual-Use-Produkt nach französischem Recht Verpflichtungen zur Speicherung der Rahmendaten der Videokonferenzen über sechs Jahre zu unterliegen. Tixeo konnte uns bis zum Redaktionsschluss dieser Hinweise nicht mitteilen, wieweit diese Verpflichtung reicht und auf welcher Rechtsgrundlage sie beruht. Verantwortliche sollten hierüber detaillierte Informationen anfordern, soweit möglich die sofortige Löschung der Rahmendaten nach Ende einer Konferenz anfordern und prüfen, ob sie einen Dienst nutzen können, der eine derartig umfassende Datenspeicherung vornimmt, für die Verantwortliche selbst regelmäßig keinerlei Rechtsgrundlage hätten.

Werk21 – BigBlueButton

Bei dem von Werk21 bereitgestellten Angebot erhalten Verantwortliche einen Zugang mit Moderationsrechten auf einer BigBlueButton-Instanz.

Teilnehmende benötigen zum Betreten der Videokonferenz in den Voreinstellungen nur die Adresse (URL) der Konferenz und betreten diese mit aktiviertem Mikrofon und deaktivierter Kamera. Verantwortliche sollten daher für die verwendeten Konferenzräume konfigurieren, dass eine Teilnahme nur für angemeldete Teilnehmende und Gäste mit Kenntnis eines zusätzlichen Zugangscodes möglich ist und dass Teilnehmende mit deaktiviertem Mikrofon die Konferenz betreten. Zusätzlich ist es möglich und ratsam einzustellen, dass eine Freigabe durch die moderierende Person erfolgen muss.

In den Voreinstellungen wird die Videokonferenz erst gestartet, nachdem die moderierende Person sie eröffnet hat. Es ist aber möglich, auch anderen authentifizierten Teilnehmenden die Eröffnung zu erlauben oder Moderationsrechte zu gewähren.

Trotz Bereitstellung einer Funktion für die Steuerung der Aufnahme wird zunächst eine Aufnahme der gesamten Konferenz vorgenommen und diese Aufnahme zu einem späteren Zeitpunkt anhand der gesetzten Schnittmarken zurechtgeschnitten. Dies kann zur Unrechtmäßigkeit der Verarbeitung führen und widerspricht in jedem Fall dem Grundsatz der Datenminimierung sowie regelmäßig den Erwartungen der nutzenden Personen. Es wird daher empfohlen, die Funktion dauerhaft zu deaktivieren.

Wir haben keine Mängel bei der Transportverschlüsselung gefunden.

Wire Pro

Im Angebot von Wire gibt es keine Möglichkeiten zur Moderation der eigentlichen Videokonferenzen. Gruppenmoderator*innen haben lediglich die Möglichkeit, andere Personen aus der Gruppe zu entfernen. Der Ausschluss einer Person aus einer Gruppe entfernt diese aber nicht aus bereits laufenden Videoanrufen.

Kontrolle über die Aktivierung/Deaktivierung der Kamera oder des Mikrofons haben die Teilnehmenden selbst. Bei mehr als zwei Personen starten die Teilnehmenden (außer der moderierenden Person) mit deaktivierten Eingabegeräte.

Da die Nutzung von Wire zur Kommunikation die Mitgliedschaft in einem Team voraussetzt, haben Verantwortliche allerdings direkte Kontrolle darüber, welche Personen im Kontext der Anwendung miteinander kommunizieren können.

Wire bietet eine starke Ende-zu-Ende-Verschlüsselung an. Die Authentifizierung der teilnehmenden Geräte erfolgt über einen Abgleich ihrer digitalen Fingerabdrücke. Ein Sicherheitsgewinn kann erzielt werden, wenn der Abgleich in persönlicher Nähe oder über einen getrennten Kommunikationskanal geschieht.

Zoom

Mängel im Auftragsverarbeitungsvertrag. Unzulässige Einschränkungen der Weisungsbindung, der Löschpflicht und der Kontrollrechte. Unzulässige Datenexporte.

Das „Zoom Global Data Processing Addendum“, November 2020 (folgend: „DPA“) führt in Ziff. 2.3 und 3.2 neu einen Verweis auf das „Zoom Privacy Statement“ ein, der es unklar macht, ob und ggf. inwiefern Zoom als Auftragsverarbeiter, als allein Verantwortlicher oder als gemeinsam Verantwortlicher mit den Kundinnen und Kunden agiert. Das „Zoom Privacy Statement“ (letzte Änderung August 2020) erklärt sich für den Fall der Auftragsverarbeitung nämlich ausdrücklich für unanwendbar.

Die Kategorien betroffener Personen in Exhibit A und Appendix 1 zu Exhibit C DPA sind unzureichend beschrieben. Es müssen abschließende konkrete Angaben gemacht werden.

Die Arten verarbeiteter Daten in Exhibit A und Appendix 1 zu Exhibit C DPA sind unzureichend beschrieben. Die Liste ist einerseits nicht abschließend, andererseits fehlen in der konkreten Aufzählung zumindest sämtliche Inhalte der Kommunikation. Diese sind zwar unter dem Begriff „Cloud Recordings“ beschrieben, aber nur in Form der Speicherung als MP4. Tatsächlich werden diese Daten auch für die Konferenz als solche verarbeitet – nur eben nicht ohne Weiteres gespeichert. Zu diesen technisch notwendig zu verarbeitenden Daten gehören jedenfalls auch die IP-Adressen der Teilnehmenden. Ob weitere Kategorien fehlen, sollte ebenfalls geprüft werden.

Die Weisungsbindung in Ziff. 3.2 DPA genügt weiterhin nicht den Anforderungen von Art. 28 Abs. 3 lit. a DS-GVO, da sie Verarbeitungen außerhalb der Weisungen auch im Fall von Verpflichtungen des Anbieters aus anderem Recht als dem der Europäischen Union oder der Mitgliedstaaten, dem der Anbieter unterliegt, erlaubt. In der Folge genügt auch die Pflicht zur Information über entsprechende Verarbeitungen nicht mehr den Anforderungen des Art. 28 Abs. 3 lit. a DS-GVO. Zu prüfen ist, ob der Verweis auf das Zoom Privacy Statement weisungswidrige Verarbeitungen erlaubt.

Ziff. 6.1 des aktuellen DPA beschränkt die Verpflichtungen zu Sicherheitsmaßnahmen nunmehr auf „Customer’s Personal Data“ und könnte so verstanden werden, dass nur die personenbezogenen Daten der Vertragspartnerinnen und Vertragspartner, nicht aber die personenbezogenen Daten, die der Anbieter im Auftrag verarbeitet, geschützt werden müssen. Dies ist jedenfalls im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) problematisch.

Ziff. 3.4 Satz 3 DPA schließt die Löschung der verarbeiteten personenbezogenen Daten nach Vertragsende in größerem Umfang aus als nach Art. 28 Abs. 3 lit. g DS-GVO zulässig, indem jedes beliebige anwendbare Recht eine Nichtlöschung rechtfertigt. Zudem enthält die Klausel einen Verweis auf die „data retention and deletion policy“ des Anbieters, die einerseits nicht Vertragsbestandteil ist, was jedenfalls im Hinblick auf die Formvorschrift des Art. 28 Abs. 9 DS-GVO und die Rechenschaftspflicht nach Art. 5 Abs. 1 lit. a, Abs. 2 DS-GVO problematisch ist, und die andererseits auch weitere unzulässige Einschränkungen der Löschpflicht beinhalten könnte, insbesondere, da offenbar ein dynamischer Verweis auf die jeweils aktuelle Policy vorliegt, sodass auch später einseitige Änderungen durch den Anbieter erfolgen könnten, über die Kundinnen und Kunden nicht einmal informiert werden müssen. Ziff. 3 Satz 4 DPA schränkt implizit die Löschpflicht sogar noch weiter ein, indem auch der Fall geregelt wird, dass die Löschung „impracticable or prohibited by law, rule or regulation“ ist. Zum rechtlichen Verbot gilt das soeben Gesagte; eine Löschung muss technisch ermöglicht werden. Ziff. 9.5 DPA könnte so verstanden werden, dass dadurch das Weisungsrecht im Fall von Datenpannen beschränkt werden soll, und sollte klargestellt werden.

Ziff. 9.7 DPA schließt die Unterstützung durch den Anbieter bei Datenpannen aus, wenn diese durch Handlungen oder Unterlassungen der Kundinnen und Kunden verursacht wurden. Der Anbieter hat zwar eine Ausnahme eingefügt, dass der Ausschluss nicht gilt, wenn das anwendbare Datenschutzrecht dies verlangt, doch verlangt Art. 28 Abs. 3 lit. f DS-GVO nicht, dass der Anbieter unterstützt, sondern nur, dass der Vertrag eine Unterstützungspflicht

vorsieht. Dies ist jedenfalls im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 1 lit. a, Abs. 2 DS-GVO) problematisch.

Ziff. 9.3 enthält zwar eine für sich genommen den Anforderungen des Art. 28 Abs. 3 lit. h DS-GVO wohl noch genügende Klausel. Allerdings enthält Ziff. 9.4 schwerwiegende Einschränkungen der Kontrollrechte der Kundinnen und Kunden, die sowohl Art. 28 Abs. 3 lit. h DS-GVO als auch den Standardvertragsklauseln widersprechen. So sind eine mindestens 30-tägige Ankündigungsfrist und eine vorherige Vereinbarung über Vor-Ort-Kontrollen ohne Ausnahme vorgeschrieben, auch in Eilfällen und mit der Möglichkeit für den Anbieter, Kontrollen durch Verweigerung der Vereinbarung zu verzögern und zu verhindern. Der Anbieter kann dritte Auditoren erlauben oder ablehnen. Vor-Ort-Kontrollen dürfen – auch bei Änderungen in der Verarbeitung, auch bei mehreren Verarbeitungsorten, auch bei schwerwiegenden Zwischenfällen – maximal einmal jährlich stattfinden. Kundinnen und Kunden haben „any additional costs arising from this“ zu tragen, was sich dem Wortlaut nach zwar nur auf die Beschränkung der Kontrollen auf einmal jährlich bezieht, dem Sinn nach aber wohl sämtliche Kontrollen meint, und zwar auch den Fall, dass diese erst durch Verschulden des Anbieters erforderlich geworden sind. Darüber hinaus enthält auch Exhibit B Ziff. 20.1 ebenfalls schwerwiegende Einschränkungen der Kontrollrechte, die teilweise den vorgenannten entsprechen, teilweise sogar darüber hinausgehen, indem jedes Kontrollrecht ausgeschlossen wird und stattdessen auf einen durch den Anbieter selbst eingeholten Audit-Report verwiesen wird, ausgenommen den Fall, dass es zu einem Sicherheitsvorfall (Security Breach) gekommen ist, der erhebliche geschäftliche Auswirkungen auf die Kundin/den Kunden hatte, oder dass ein Audit-Recht gesetzlich vorgeschrieben ist. Letzteres ist im Anwendungsbereich der DS-GVO nicht der Fall, sondern Art. 28 Abs. 3 lit. h DS-GVO schreibt nur vor, dass der Auftragsverarbeitungsvertrag vertraglich ein Audit-Recht vorsehen muss.

Ziff. 5.2 DPA sieht eine pauschale Genehmigung von Sub-Auftragsverarbeitern vor, die auf einer WWW-Seite aufgeführt sind, was jedenfalls im Hinblick auf die Rechenschaftspflicht problematisch ist, aber auch im Hinblick auf Art. 28 Abs. 2 DS-GVO zweifelhaft ist. Die Liste der Subunternehmer zum Zeitpunkt des Vertragsschlusses muss nicht mit einer eventuell durch die Verantwortlichen gesichteten und/oder gesicherten Fassung übereinstimmen, und es nicht einmal geregelt, ob relevanter Zeitpunkt derjenige der Unterzeichnung durch die Verantwortlichen ist oder derjenige der Unterzeichnung durch Zoom. Damit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) nachkommen. Die auf der angegebenen WWW-Seite aufgeführten Sub-Auftragsverarbeiter sind zudem nicht ordnungsgemäß benannt, in den meisten Fällen nicht einmal mit ihrem vollständigen Namen, in jedem Fall ohne Anschrift. Die Aufgabenbereiche sind nicht klar abgegrenzt, und die Angaben auf der WWW-Seite stimmen nicht mit den Angaben überein, die der Anbieter uns gegenüber gemacht hat, was die Bedeutung einer schriftlichen Fixierung der zugelassenen Sub-Auftragsverarbeiter unterstreicht.

Das Verfahren zur Information über neue Unterauftragsverarbeiter in Ziff. 5.3.1 Satz 3 DPA erfordert ein aktives Handeln der Verantwortlichen und genügt damit nicht Art. 28 Abs. 2 Satz 2 DS-GVO. Verantwortliche, die die Benachrichtigungen nicht selbst aktiv abonnieren, können zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 5.3.2.d) DPA macht es Verantwortlichen faktisch unmöglich, gegen neue Unterauftragsverarbeiter Einspruch einzulegen, weil sie und der Anbieter nur ein Kündigungsrecht für das DPA haben, wenn der Anbieter keine alternative Lösung anbietet, aber ihre Zahlungsverpflichtungen nach dem Hauptvertrag fortbestehen. Der Anbieter kann zudem einseitig die Leistung einstellen, Ziff. 5.3.2.d) DPA. Dies entwertet das Einspruchsrecht vollständig, sodass ein Verstoß gegen Art. 28 Abs. 2 Satz 2 DS-GVO vorliegt. Darüber hinaus beträgt die Widerspruchsfrist gegen neue Sub-Auftragsverarbeiter nur zehn Tage.

Ziff. 5.5 verstößt gegen Art. 28 Abs. 4 S. 1 DS-GVO, weil in der aktuellen Fassung – anders als in früheren Fassungen – Sub-Auftragsverarbeitern nicht mehr dieselben Datenschutzpflichten auferlegt werden müssen, sondern nur noch gleichwertige. Zudem sind entgegen

Art. 28 Abs. 4 S. 1 DS-GVO auch andere Rechtsinstrumente als nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zugelassen.

In Ziff. 5.7 DPA werden die Standardvertragsklauseln unzulässig abgewandelt, sodass diese den Datenexport nicht rechtfertigen können (unabhängig von der Frage, ob diese Abwandlung zivilrechtlich wirksam ist oder nicht).

Ziff. 10.4 DPA gibt dem Anbieter das einseitige Recht zur Vertragsänderung unter bestimmten Bedingungen.

Aufgrund der rechtlichen Mängel erfolgte keine technische Prüfung.

Prüfpflichten der Verantwortlichen

Auch wenn unsere Prüfungen keine Mängel aufgedeckt haben, bedeutet dies nicht, dass diese nicht vorliegen und entbindet Verantwortliche nicht von ihren gesetzlichen Pflichten. Es wird ausdrücklich darauf hingewiesen, dass keine umfassende Prüfung der Angebote erfolgte, insbesondere keine umfassende technische Prüfung und in der Regel auch keine Prüfung der Datenschutzerklärungen. Letztere betreffen lediglich die eigenverantwortlichen Datenverarbeitungen der Videokonferenzsystem-Anbieter. Nicht von den Datenschutzerklärungen umfasst sind diejenigen Datenverarbeitungen, die verantwortliche Stellen mit Sitz in Berlin durchführen, wenn sie die Dienste in Anspruch nehmen.

Wir empfehlen den Verantwortlichen daher insbesondere Folgendes zu prüfen:

- Hat sich der Auftragsverarbeiter entgegen der Festlegungen in dem von uns geprüften Vertragswerk anderweitig die Verarbeitung der Nutzungsdaten zu eigenen Zwecken oder Zwecken Dritter vorbehalten?
- Gibt es Indizien dafür, dass sich der Auftragsverarbeiter nicht an die Festlegungen im Auftragsverarbeitungsvertrag hält?
- Nimmt der Auftragsverarbeiter ein Nutzer-Tracking vor, das für den Betrieb der Lösung nicht erforderlich ist?
- Finden sich in den Datenschutzerklärungen, die den Konferenzteilnehmer*innen im Zuge der Konferenzteilnahme durch den Auftragsverarbeiter präsentiert oder zugänglich gemacht werden, Hinweise auf eine Datenverarbeitung des Auftragsverarbeiters, die mit der vereinbarten Datenverarbeitung im Auftrag nicht in Einklang zu bringen ist?
- Ist die Sicherheit der verarbeiteten Daten und die Einhaltung von Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen auch unter den konkreten geplanten Einsatzumständen gegeben?
- Hat der Auftragsverarbeiter ausreichende Garantien für die Vornahme angemessener technischer und organisatorischer Maßnahmen bei dem Betrieb des Dienstes vorgelegt?

Fortlaufende Aktualisierung der Anbieterliste

Die Liste der Anbieter von Videokonferenzlösungen wird laufend ergänzt, wenn im Rahmen unserer Aufsichts- und Beratungstätigkeit weitere Angebote geprüft wurden. Änderungen, die uns aufgeführte Anbieter mitteilen, werden wir prüfen und in der Folgeversion berücksichtigen. Wir ermuntern zudem ausdrücklich Anbieter, die ihre Videokonferenzlösungen Berliner Verantwortlichen anbieten möchten und über besondere technische Lösungen verfügen – etwa mit Ende-zu-Ende-Verschlüsselung, mit Einbindung in professionelle User-Management-Systeme oder für eine Vielzahl von Teilnehmenden – uns über ihr Angebot zu informieren und uns die Vertragsdokumente und einen Test-Zugang zur Verfügung zu stellen. Wir bitten jedoch, vor einer Einreichung selbstkritisch zu prüfen oder durch die/den betriebliche*n Datenschutzbeauftragte*n oder Angehörige der rechtsberatenden Berufe prüfen zu lassen, ob die Verträge den gesetzlichen Anforderungen entsprechen. Hierzu empfehlen wir auch die Lektüre der Anmerkungen zu den bereits geprüften Verträgen sowie unserer „Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenzdiensten“.²¹ Diese kann Verantwortlichen auch die Prüfung der Verträge von Anbietern, die bisher nicht in der Liste enthalten sind, erleichtern. Ebenfalls bitten wir, eine technische Überprüfung des Videokonferenzdienstes entsprechend der Orientierungshilfe der DSK vorzunehmen. Identifizierte Mängel sollten vor Einreichung der Unterlagen bei uns beseitigt werden.

²¹ https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BInBDI-Empfehlungen_Pruefung_Auftragsverarbeitungsvertraege_Videokonferenz-Dienste.pdf.