Zoom kann für die dienstliche Kommunikation in Lehre, Forschung und Verwaltung nur eingesetzt werden, wenn die nachfolgend aufgeführten Mängel nachweislich geheilt wurden. Siehe hierzu auch die Veröffentlichung der Berliner Beauftragten für Datenschutz und Informationsfreiheit, zu finden unter „Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten“
https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/corona-pandemie/

Zoom – Rechtliche Mängel

(Hier: Insbesondere Mängel im Auftragsverarbeitungsvertrag)

Unzulässige Einschränkung der Löschpflicht und Rechenschaftspflicht

- Ziff. 3.4 Satz 1 des „Zoom Global Data Processing Addendum“, December 2019 (folgend: „DPA“) schließt die Löschung der verarbeiteten personenbezogenen Daten nach Vertragsende in größerem Umfang aus als nach Art. 28 Abs. 3 lit. g DSGVO zulässig, indem jedes beliebige auf Zoom bzw. Unterauftragsverarbeiter anwendbare Recht eine Nichtlöschung rechtfertigt.
- Ziff. 3.4 Satz 2 und Ziff. 4.3 DPA könnten als Spezialregelungen Ziff. 6 DPA vorgehen, widersprechen jedenfalls Ziff. 6 DPA. Ziff. 6 DPA darf allerdings nicht eingeschränkt werden, da sonst ein Verstoß gegen Art. 32 DSGVO vorliegen würde. Damit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 lit. a DSGVO) nachkommen.

Unzulässige Regelungen zu Subunternehmern (weiteren Auftragsverarbeitern) sowie Entwertung von Einspruchsrechten

- Ziff. 5.1 Satz 1 DPA verweist für den Einsatz von weiteren Auftragsverarbeitern auf einen URL, der eine Liste genehmigter Unterauftragsverarbeiter enthält, und sieht insoweit einen Aktualisierungsvorbehalt vor, wobei nicht eindeutig ist, ob sich der Aktualisierungsvorbehalt auf URL oder Inhalt beziehen soll. Durch diese Unklarheit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DSGVO) nachkommen.
- Darüber hinaus muss die Liste der Subunternehmer zum Zeitpunkt des Vertragsschlusses nicht mit einer eventuell durch den Auftraggeber gesichteten und/oder gesicherten Fassung übereinstimmen, und es nicht einmal geregelt, ob relevanter Zeitpunkt derjenige der Unterzeichnung durch den 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.
- Das Verfahren zur Information über neue Unterauftragsverarbeiter in Ziff. 5.1 Satz 2 und 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. 5.2.1 DPA macht es Verantwortlichen faktisch unmöglich, gegen neue Unterauftragsverarbeiter Einspruch einzulegen, weil sie nur ein Kündigungsrecht für das DPA haben, aber ihre Zahlungsverpflichtungen nach dem Hauptvertrag fortbestehen. Dies entwertet das Einspruchsrecht vollständig, sodass ein Verstoß gegen Art. 28 Abs. 2 Satz 2 DS-GVO vorliegt.

Unzulässige Einschränkung von Kontrollrechten (insb. Vor-Ort-Kontrolle)

- Ziff. 9.3 und 9.4 DPA verstoßen gegen Art. 28 Abs. 3 lit. h DS-GVO. Es besteht keine umfassende Verpflichtung für Zoom, Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen. Das einzige Recht, das es (unzulässig eingeschränkt, weil stets eine Vorankündigung verlangt wird, auch im Eilfall, und nur einmal jährlich, auch wenn zwischenzeitlich die Verarbeitung geändert wurde) gibt, ist das, sich Unterlagen im Büro von Zoom anzuschauen; außerdem maximal einmal jährlich eine Kopie nicht näher bezeichneter Zertifikate/Reports. Jegliches Recht zu eigenen Überprüfungen, die über die Einsicht in Unterlagen hinausgehen, insbesondere zur Vor-Ort-Kontrolle, ist ausgeschlossen.

Unzulässige Datenexporte

- In Ziff. 3.4 letzter Satz, 5.6 am Ende und 9.4 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). Die Selbstzertifizierung nach dem Privacy Shield bezieht sich nicht auf persbez. Daten.

Zoom – Technische Mängel

Der Anbieter Zoom ist in der Vergangenheit mehrfach durch Sicherheitspannen, vor allem aber durch den teils verschleiernden Umgang mit Sicherheitsvorfällen aufgefallen. Die Meldungen über eklatante Fehler bei Zoom reißen nicht ab und werden auch außerhalb der Fachpresse öffentlich diskutiert. Eine (nicht vollständige) Auswahl einiger bislang veröffentlichter (und teilweise inzwischen behobener) Sicherheitslücken, die Aufschluss über die Qualität des Dienstes gibt:

- Fehler in der Windows-Version von Zoom ermöglichten unter anderem den Diebstahl von Windows-Benutzerdaten.
- Die Mac-Version von Zoom nutzte Schadsoftware-Technik, um sich zu installieren.
- Beim Start übertrug Zoom in der IOS-App personenbezogene Daten an Facebook und glich Nutzerdaten mit LinkedIn ab - in beiden Fällen wurde darauf in der Datenschutzerklärung nicht hingewiesen und die Zustimmung der Nutzer_innen nicht eingeholt.
- Die Standardeinstellungen schützten Gespräche nicht vor unerwünschten Teilnehmenden. Deshalb kämpften Zoom-Nutzer_innen immer wieder mit Belästigungen, dem so genannten „Zoombombing“ (z.B. das Einblenden von pornographischem Material und Missbrauchsdarstellungen in Videokonferenzen).
- Kamera-Aktivierung auf Apple-Geräten durch einen undokumentierten Webserver, der auch nach manueller Deinstallation noch ansprechbar war, ohne dass die Nutzer_innen dies bemerkten. Dies wurde von Apple durch ein sogenanntes „Silent Update“ (sehr ungewöhnliche Maßnahme seitens Apple, verweist auf die Schwere des Risikos) behoben.
- Zoom sammelt unnötig viele Daten, die für das Anbieten des Videokonferenz-Services nicht nötig sind, und die ein "Profiling", also ein Ausspähen der Nutzer_innen ermöglichen. Hierfür gelten in Europa strenge Richtlinien, die wir nur durch ein Löschen der gesammelten Daten, eine Beschränkung der Zugriffsrechte auf diese Daten und die Einhaltung von datenschutzkonformen Voreinstellungen gewährleisten können. Dies können wir aber aufgrund der bislang angebotenen mangelhaften Auftragsverarbeitungsverträge (sieh oben) und dem Verarbeitungsort USA aktuell nicht kontrollieren.
- Darüber hinaus ermöglicht Zoom eine Kontrolle der Meetings sowie der Teilnehmenden und deren Profiling durch weitreichende Admin-Rechte. So ermöglicht das Dashboard für den Admin unter anderem:
  - (für Meeting-TN und Hosts unbemerkten) Echtzeitzugriff auf alle Meetings, Aufzeichnungen, Chatprotokolle
  - Auswertungen und Rankings (z.B. TopUser) sowie Weiterverarbeitung dieser „Auswertungen“ durch Download
  - Informationen über genutzte Betriebssysteme, IP-Adresse, Standortdaten und Geräteinformationen jedes Teilnehmers inkl. Gerätetyp (PC/Mac/Linux/Mobile/etc.), Angaben zur Marke/Modell und ihrer audiovisuellen Peripheriegeräte wie Kameras oder Lautsprecher sowie die Namen für diese Geräte (z.B. die vom Benutzer konfigurierbaren Namen, die AirPods erhalten).
  - Das so genannte „Attendee Attention Tracking“, d.h. wenn das Zoom-Fenster der Teilnehmenden für 30 Sekunden nicht im Vordergrund ist, erhält der Host einen Hinweis.

Zoom – Grundsätzliches Problem: Datenverarbeitung außerhalb EU/EWR

- Siehe hierzu: Pressemitteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/17_Schrems-II-Urteil.html

- Sowie Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit (unsere Aufsichtsbehörde) unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf