Projekt Rechtsinformationsstelle Digitale Hochschule NRW

Leitung: Prof. Thomas Hoeren

Bearbeiter:innen: Wissenschaftliche Mitarbeiter:innen Julian Albrecht, Malin Fischer, Owen Mc Grath, Nicolas John, Maximilian Wellmann

Veröffentlicht am 18. Mai 2020

Fragestellung

Können Universitäten für den Lehr- und Arbeitsbetrieb den Videokonferenzdienst des Unternehmens Zoom Inc. DSGVO-konform anbieten? Wenn ja, was ist bei der Auswahl und Einrichtung von Zoom zu beachten?

Hintergrund

Die Corona-Krise erfordert ein in weiten Teilen „digitales Sommersemester“, welches die Hochschulen in NRW ad hoc organisieren müssen, teilweise ohne sich zuvor stark mit der Digitalisierung der Lehre beschäftigt zu haben.

Als erster Schritt ist vielerorts die Einrichtung eines Videokonferenzsystems erforderlich, mit dem die Möglichkeit geschaffen wird, persönliche Treffen in die digitale Sphäre zu verlagern, und im Lehrbetrieb synchrone Lehrelemente zu ermöglichen (z.B. Arbeitsgruppen, Seminare, interaktive Teile der Vorlesung) (abzugrenzen von Programmen, die die Aufzeichnung asynchroner Lehrelemente, sog. Videokonserven, ermöglichen).

Inhalt

Kurzantwort und praktisches Vorgehen

Aus unserer Sicht ist es für Hochschulen möglich, unter Beachtung einiger Verhaltensweisen Zoom DSGVO-konform einzurichten und fortlaufend anzubieten.

Die Hochschule ist bei Einrichtung und Anbieten eines Videokonferenzdienstes Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO und muss damit gegenüber den Nutzern als auch gegenüber der zuständigen Aufsichtsbehörde für eine ausreichende Gewähr der DSGVO-Vorgaben einstehen. Praktisch lässt sich dies unseres Erachtens unter Zusammenarbeit der Hochschul-Datenschutzbeauftragten und des entsprechenden IT-Teams erreichen durch die folgenden zehn Schritte:

1. Abwägungsentscheidung bei der Auswahl eines Videokonferenzdienstes als Auftragsverarbeiter unter Berücksichtigung von Alternativen dokumentieren.

2. Abschluss eines Auftragsverarbeitungsvertrags (AVV) mit Zoom Inc., welcher von Zoom bereitgestellt wird.

3. Abschluss der dem AVV angehängten Standard Contractual Clauses (SCC).

4. Implementierung der Software in das Hochschule-IT-System durch die Hochschul-IT-Abteilung und dabei Deaktivierung gewisser Funktionen und Programmstrukturen.

5. Vornahme datensparsamer Voreinstellungen (defaults) durch die Hochschul-IT-Abteilung.

6. Erstellung einer eigenen Datenschutzerklärung.

7. Erstellung von Anleitungen und Schulungsunterlagen für NutzerInnen zur datenschutzfreundlichen Nutzung von Zoom, etwa inkl. Sicherheitshinweise bzgl. Zoombombing, ggfs. in Zusammenarbeit mit anderen Hochschulen.

8. Ergänzung des Datenverarbeitungsverzeichnises gem. Art. 30 DSGVO um die Datenverarbeitungen in Zusammenhang mit Zoom.

9. Zusendenlassen der Verträge von Zoom mit Unterauftragsverarbeitern („Subprocessors“) und Anlage einer entsprechenden Liste.

- Freischaltung des Angebots -

10. Während des Betriebes

    a. Monitoring der ggfs. neu hinzukommenden Unterauftragsverarbeitern und ggfs. Widerspruch bei bekannten Mängeln des Unterauftragsverarbeiters (dann werden Alternativen, wenn nicht möglich Vertragsauflösung angeboten)

    b. Anfordern und Durchsicht der jährlichen Datensicherheits-Auditierungen bei Zoom

Gang der Untersuchung und Methodik

Letzte Woche haben wir eine erste Einschätzung zur Möglichkeit der rechtskonformen Nutzung von Zoom durch Hochschulen veröffentlicht. Darin haben wir uns auf die öffentlich gewordenen Sicherheitslücken bei Zoom und andere datenschutzrechtliche Kritik konzentriert und analysiert, ob Abhilfe geschaffen wurde (Ergebnis: größtenteils ja). Zudem haben wir die bis dato veröffentlichte (teilweise graue) Literatur gesichtet. Diese kommt weitgehend zu dem Ergebnis, dass eine DSGVO-konforme Nutzung mit gewissen Vorkehrungen möglich ist. Landesdatenschützer empfehlen verbreitet, grundsätzlich von der Nutzung amerikanischer kommerzieller Dienste abzusehen, verneinen aber nicht per se die Möglichkeit einer rechtskonformen Nutzung. Wir sind zu der ersten Einschätzung gelangt, dass ein DSGVO-konformes Angebot von Zoom durch Hochschulen an ihre Angehörige unter Beachtung gewisser Punkte möglich ist.

Nunmehr haben wir die Datenschutzrichtlinie von Zoom und den von Zoom angebotenen vorformulierten Auftragsverarbeitervertrag iSd Art. 28 DSGVO („Data Processing Addendum“) inklusive Anhängen (Beschreibung technisch-organisatorischer Maßnahmen; Standard Contractual Clauses i.S.d. Art. 46 Abs. 3, 28 Abs. 8 DSGVO) durchgearbeitet. Wir haben unter Berücksichtigung rechtswissenschaftlicher Literatur geprüft, ob die Vorgaben der DSGVO erfüllt werden. Dabei mussten wir unterstellen, dass die Pflichten von Zoom wie in den Verträgen und Erklärungen festgelegt auch praktisch von Zoom Inc. so umgesetzt werden. *Dies zu überprüfen obliegt den Verantwortlichen („FILL IN DSGVO“) (den Hochschulen) im Rahmen ihrer Möglichkeiten (siehe unten) und kann von der rechtlichen Prüfung hier nicht geleistet werden.* Im Austausch mit der WWU.IT konnten wir erfahren, wie der Ablauf der Einrichtung von Zoom bei institutionellen Kunden wie Hochschulen funktioniert.

Übersicht zur datenschutzrechtlichen Konstellation beim Angebot von Zoom durch eine Hochschule

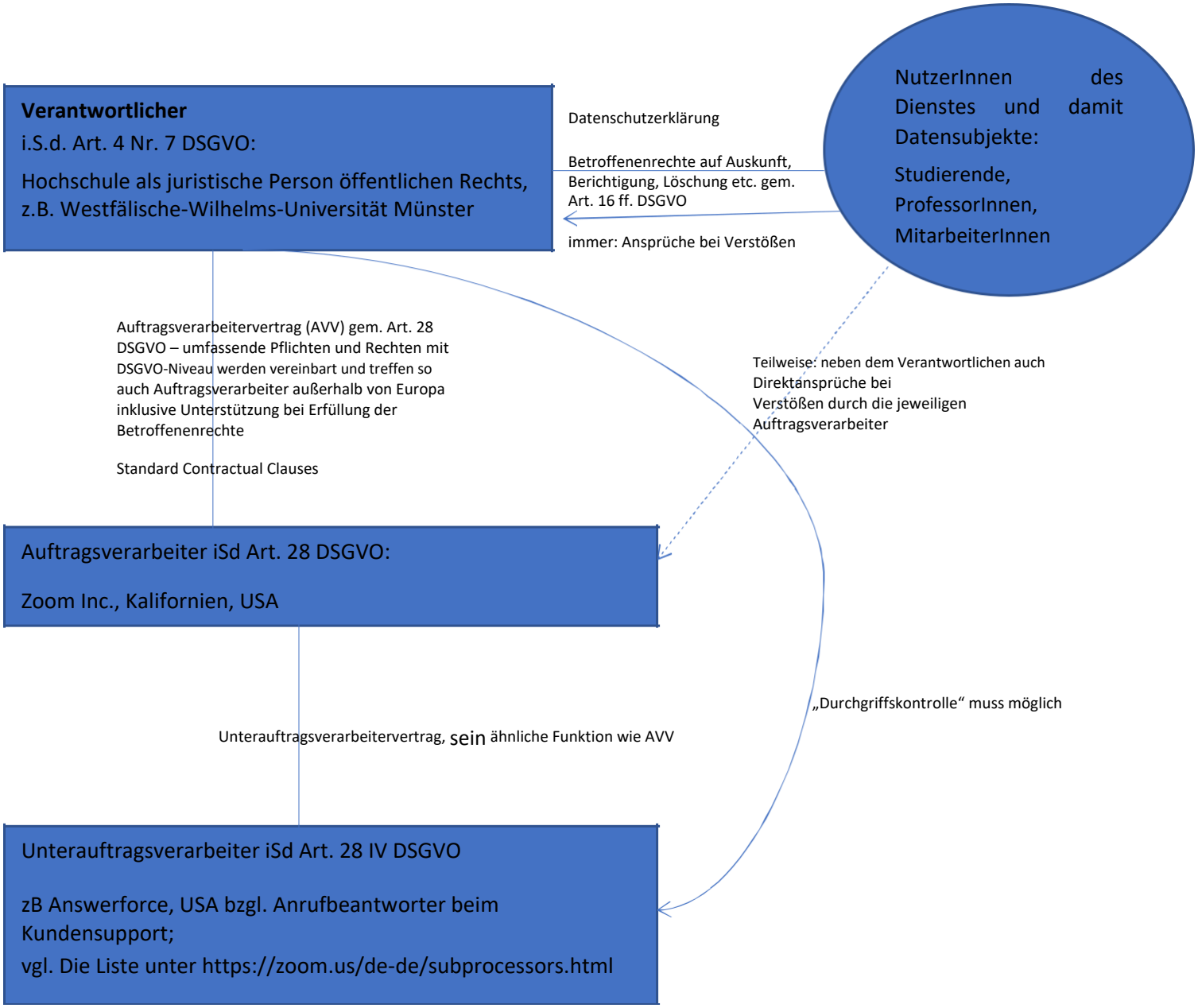

Abb.1:

Hochschulen haben bei der Einrichtung von Zoom in ihren IT-Strukturen die Möglichkeit, Zoom zu konfigurieren und z.B. einzelne Funktionen von Zoom oder Einstellungsmöglichkeiten ganz zu deaktivieren und im Übrigen die Voreinstellungspositionen („defaults“) anzupassen. Damit und mit der Auswahl von Zoom als Diensteanbieter überhaupt bestimmt die Hochschule „Zweck und Mittel“ der Datenverarbeitung und wird zum Verantwortlichen der Datenverarbeitung.

Zoom Inc. ist in dieser Konstellation (in Abgrenzung zur rein privaten Nutzung von Zoom ohne zwischengeschaltete Institution) Auftragsverarbeiter i.S.d. Art. 28 DSGVO. Es ließe sich auch argumentieren, dass Zoom Inc. als Anbieter eines komplexen und vollständig funktionalen Cloud-4

Services aufgrund der tatsächlich größeren Einflussmöglichkeiten, was die konkrete technische Umsetzung der Datenverarbeitung angeht (Serverstrukturen, Skripte etc.) eigentlich neben einer Hochschule gemeinsamer Verantwortlicher i.S.d. Art. 26 DSGVO ist. Die vertragliche Ausgestaltung im Fall von Zoom (der von Zoom vorgegeben AVV) als auch die verbreitete Praxis in Deutschland, was Cloud-Services angeht, versteht Zoom Inc. aber als Auftragsverarbeiter.

Praktisch bestehen unseres Erachtens wenig Unterschiede der beiden Einordnungen. Gravierendste Konsequenz ist, dass NutzerInnen des Hochschul-Zoom-Dienstes sich mit Auskunfts-, Löschungs-, Berichtigungsersuchen und Ähnliches nicht direkt an Zoom wenden können, sondern über die Hochschule vorgehen müssen. Zoom Inc. ist indes im Innenverhältnis gegenüber der Uni über den AVV umfangreich Rechenschaft schuldig und muss etwa bei den genannten Ersuchen technisch-organisatorische Maßnahmen vorhalten, damit die Verantwortliche die Anfragen beantworten kann. Auch als Auftragsverarbeiter haftet Zoom Inc. im Übrigen für rechtswidrige Datenverarbeitungen sowohl im Innenverhältnis ggü. der Hochschule als auch im Außenverhältnis gegenüber dem Endnutzer für rechtswidrige Datenverarbeitungsvorgänge nach Art. 28 Abs. 10, 82 DSGVO.

Detailliertere Prüfungsergebnisse zu den Schritten 1.-10.

Unsere Arbeit hat die letzte Woche veröffentlichte erste Einschätzung bestätigt. Unseres Erachtens kann unter Berücksichtigung verschiedener Verhaltensweisen die IT-Abteilung einer Hochschule in Zusammenarbeit mit dem Datenschutzbeauftragten ein Hochschul-Zoom DSGVO-konform ihren Angehörigen anbieten.

Schritt 1: Eine dokumentierte Abwägungsentscheidung bei der Auswahl eines Videokonferenz-dienstes als Auftragsverarbeiter unter Berücksichtigung von Alternativen, Art. 25 Abs. 1, 28 Abs. 1 DSGVO

Die Entscheidung allgemein für die Anschaffung einer Videokonferenzsoftware als auch bei der Auswahl einer konkreten Software muss unter Abwägung der folgenden Kriterien erfolgen, die Art. 25 Abs. 1, 28 Abs. 1 DSGVO zu entnehmen sind:

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen
- Vorliegen hinreichender Garantien von dem Auftragsverarbeiter für die Durchführung und das Vorhalten geeigneter technischer und organisatorischer Maßnahmen zur DSGVO-konformen Datenverarbeitung
- Fachwissen, Zuverlässigkeit, Ressourcen des Auftragsverarbeiters

Die Vorgaben von Art. 25 Abs. 1, 28 Abs. 1 DSGVO sind dabei so zu verstehen, dass ein Mindestmaß an Datenschutz nicht unterschritten werden darf. Hingegen muss nicht pauschal die optimale 5

datenschutzrechtliche Lösung gewählt werden. Neben den Aspekten der Datensicherheit stehen die Zwecke der Verarbeitung als gleichrangige Abwägungskriterien.
Dafür, dass nach Abwägung der Kriterien eine Entscheidung auf Zoom fallen kann, spricht:

- Zoom es leisten, Meetings auch mit mehreren Hundert Teilnehmern mit hinreichender Qualität (Bildqualität, Latenz) zu übertragen – nach verbreiteter Auffassung *anders als* OpenSource-Systeme wie z.B. BigBlueButton oder JitsiMeet.

- Zoom bietet einige für Lehrveranstaltung besonders nützliche („erforderliche“) Funktionen wie z.B. das Handheben, andere Reaktionen, welche von anderen Systemen nicht angeboten werden.

- Die Implementierungskosten sind überschaubar. Zu den Implementierungskosten zählen auch der Personalaufwand durch (IT-)Mitarbeiter bei der Einrichtung des Systems.

- Die Schwere der Risiken für Rechte und Freiheiten natürlicher Personen bei Eintritt eines Verarbeitungsverstoßes kann verringert werden, soweit Zoom „nur“ für Anwendungsfälle verwandt wird, in denen keine besonders sensiblen Daten verarbeitet werden, z.B. nicht bei Prüfungsgesprächen oder Diskussion neuester Forschung. (unter dem Vorbehalt des nächsten Punktes.)

- In unserem ersten Papier zu Zoom („20_05_01_Zusammenfassung Zoom und erste rechtliche Bewertung.pdf“) haben wir vorgeschlagen, den Einsatz von Zoom auf den Anwendungsfall besonders großer Meetings (mehr als 50 Teilnehmer) mittelfristig zu beschränken und für kleinere Gruppen ein datensparsameres und zwar weniger performantes, für diese Zwecke aber hinreichend performantes System anzubieten (z.B. BigBlueButton, JitsiMeet). An dieser Stelle hatten wir die Frage offengelassen, inwieweit „Reibungsverluste“ durch das Eingewöhnen-Müssen verschiedener Akteure in mehr als einem Programm in eine Abwägung eingestellt werden könnte etwa unter dem Kriterium der Implementierungskosten.

  Wir haben diese Frage inzwischen untersucht und konnten in der Literatur keine Stimme finden, die sich überhaupt mit dieser Frage befasst hätte. Ausnahmslos scheinen die AutorInnen für *einen* Anwendungsbereich einer Datenverarbeitung auch den Einsatz *einer* Software für selbstverständlich zu erachten – auch für ressourcenstarke Institutionen wie zum Beispiel große Universitäten. Natürlich verschiebt sich die Frage dann in den Bereich der Definition des „Anwendungsbereiches“. Es erscheint jedoch zumindest vertretbar, das Angebot von synchronen Videokonferenzen insgesamt als Anwendungsbereich zu definieren, ohne nach Quantität der Teilnehmer oder Sensibilität der Daten zu differenzieren.

  Daraus ergibt sich, dass wir nun zu der Einschätzung gelangen, dass das Angebot eines zweiten Videokonferenzdienstes neben Zoom mit oben genannter Überlegung zwar vorbildlich, nicht aber rechtlich geboten ist. (Ein praktischer Mittelweg könnte sein wie die Uni Münster neben dem allgemeinen Zoomdienst, eine kleinere Zoom-Applikation für sensiblere Meetings anzubieten, welche OnPremises gehostet wird.)

- **Speziell zu den „hinreichenden Garantien für die Durchführung und das Vorhalten geeigneter technischer und organisatorischer Maßnahmen zur DSGVO-konformen Datenverarbeitung bei Zoom als Auftragsverarbeiter“ als Abwägungskriterium:**

    - Bei Einrichten der Software durch eine Hochschule als Administrator können nahezu alle Einstellungen als Default gesetzt, gesperrt oder ausgeschaltet, also etwa auch ganze Funktionen vollständig deaktiviert werden. Dies war zum Beispiel vor globalem Deaktivieren durch Zoom für die Funktion des Aufmerksamkeitstrackings relevant. (Eine Funktion, bei der das Zoom-Programm fortwährend prüfte, ob Teilnehmer die Anwendung im Vordergrund oder Hintergrund des Desktops laufen ließen mit entsprechender Benachrichtigung bei längerer Anwendung im Hintergrund. Sie ermöglichte dem Host indes keinen Zugriff auf die Geräte der Teilnehmer.)

    - Bezüglich der Voreinstellungen lassen sich konsequent datensparsame Voreinstellungen treffen.

      NutzerInnen von Zoom sollten weiterhin in der Nutzung geschult werden, damit sie zweckangepasste Einstellungen für ihre individuellen Meetings treffen (und etwa nicht pauschal alle datenintensiven Einstellungen wieder aktivieren). Auch das Phänomen des „Zoombombings“ lässt sich so unter Kontrolle bringen (Warteraum aktivieren, Meeting-Passwörter, Bildschirm teilen nur nach Anfrage an den Host möglich u.A.).

    - Untersuchungsgegenstand für konkrete Datenflüsse und -verarbeitungsvorgänge bei Zoom waren für uns die Datenschutzhinweise von Zoom (in der Version „Stand 29. März 2020, abzurufen unter https://zoom.us/de-de/privacy.html), der Auftragsverarbeitervertrag mit Zoom („Data Processing Addendum“, von Zoom bereitgestellt, abzurufen unter https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf) sowie die Anhänge des AVV (insb. Exhibit B „ZOOM MINIMUM SECURITY CONTROL REQUIREMENTS“). Außerdem haben wir die Presse rund um konkrete Sicherheitslücken bei Zoom ausgewertet und verfolgt wie Zoom darauf reagiert hat.

      Was die Untersuchung durch uns nicht leisten kann: Wir mussten unterstellen, dass Zoom Inc. praktisch so arbeitet wie im AVV und den Datenschutzhinweisen festgelegt bzw. bekundet. **Dies auch auf tatsächlicher Ebene in einem gewissen Rahmen zu überprüfen, obliegt den Verantwortlichen (den Hochschulen). Dies kann z.B. durch Sichtung von Exhibit B zum AVV „ZOOM MINIMUM SECURITY CONTROL REQUIREMENTS“ in Abgleich mit einem Auditbericht durch einen Informatiker der IT-Abteilung der Hochschule geschehen. (Der Auditbericht (SOC 2 Type II) wurde von einem unabhängigen Sachverständigen in den USA durchgeführt. Zoom Inc. stellt den Bericht bei Interesse an einem Vertragsschluss nach Abschluss einer Geheimhaltungsvereinbarung zur Verfügung). Diese Beurteilung fällt aus Sicht der WWU.IT positiv aus.**

    - **Datenschutzrichtlinie von Zoom**

        - Die „Datenschutzrichtlinie“ von Zoom ist in der hier geprüften Konstellation (Hochschule bietet Zoom an) keine nach außen wirksame Datenschutzerklärung eines Verantwortlichen (diese muss die Uni stellen,

siehe Übersicht oben), gibt aber Aufschluss über die Arbeitsweisen und auf einer oberflächlichen Ebene über die Datenverarbeitung bei Zoom. Vorausgesetzt Zoom hält sich an die aufgestellten Vorgaben (siehe soeben), findet sich hier kein Grund, Zoom datenschutzrechtlich ein schlechtes Zeugnis auszustellen.

Vergleiche speziell zur Auswertung der Datenschutzrichtlinie von Zoom folgendes von uns erstellte und bereits veröffentlichte Dokument: Zoom Datenschutzhinweise Kommentar final.pdf

- Einige Auszüge:

  - Es ist zwischen der Website zoom.us und den Zoom-Videokonferenzdiensten zu unterscheiden.

  - Für die Website nutzt Zoom Cookies, um die Effizienz der Webseite zu steigern und Werbeaktivitäten gegenüber (potentiellen) Kunden zu steigern. Dabei werden personenbezogene Daten verarbeitet. Es wird ausführlich darüber aufgeklärt und auf der Website selbst besteht eine opt-out Option, die prominent angezeigt wird, sobald man zum ersten Mal auf die Seite geht. Insgesamt ist das Vorgehen rechtlich als marktüblich und datenschutzrechtlich in Ordnung zu bewerten.

  - Die Datenverarbeitungen im Zusammenhang mit den Zoom-Videokonferenzdiensten (im Folgenden nur: Zoom) ist für die hier zu überprüfende Konstellation entscheidend. Angehörige der Hochschulen müssen zur Nutzung von Zoom nicht mit der Marketing-Website interagieren.

    - Datenverarbeitungen im Zusammenhang mit Zoom werden recht ausführlich und verständlich dargestellt.

    - Es wird ausdrücklich klargestellt, dass kein Verkauf der Inhaltsdaten von Konferenzen stattfindet. Gleichfalls analysiert Zoom Inc. selbst nicht die Inhaltsdaten zu Werbezwecken. Unterauftragsverarbeiter sind vertraglich dazu verpflichtet, Daten lediglich zu Vertragszwecken zu verarbeiten; eine sonstige Verwertung ist ausdrücklich untersagt.

    - Unterauftragsverarbeiter werden eingesetzt für unterstützende Services wie z.B. Buchhaltung, Support

    - Kritisch zu sehen in Bezug auf den Untersuchungszweck hier: Speicherdauer nur knapp und oberflächlich angegeben.

- **AVV**

  - Für den zu diesem Schritt relevanten Untersuchungszweck ergibt sich aus dem AVV nichts Weitergehendes, vgl. aber Schritt 2.

- **Presse rund um konkrete Sicherheitslücken bei Zoom und Reaktion von Zoom inklusive Updates mit Version 5.0 und höher**

  vgl. hierzu ausführlich die folgenden bereits veröffentlichten Dokumente:

  20_05_01_Zusammenfassung Zoom und erste rechtliche Bewertung.pdf Zoom Zusammenfassung5 1505.pdf

  einige Auszüge

  - Schnelle und vorbildliche Reaktion auf alle Sicherheitsprobleme, die öffentlich geworden sind z.B. bzgl. einem kritischen Facebook-Software-Development-Kits oder dem Rendern von UNC Links.

  - Transportverschlüsselung entspricht mit dem Update aller Teilnehmer auf Zoom 5.0 oder neuer (ab Ende Mai 2020 obligatorisch; nach jedem Meeting schon jetzt zum Update aufgefordert) jetzt dem 256-AES Standard, welcher als Stand der Technik angesehen werden kann (zuvor nur 128-AES).

  - Eine Ende-zu-Ende-Verschlüsselung der Videokonferenz-Inhalte ohne Zugriffsmöglichkeit von Zoom wird noch nicht geleistet. Nach verbreiteter Einschätzung kann eine solche Verschlüsselung wegen der Komplexität bei Vielpersonen-Videokonferenzen jedoch nicht als Stand der Technik gewertet werden.

    Kürzlich hat Zoom die Implementierung dieser Verschlüsselungsart dennoch als Ziel ausgegeben und zu diesem Zweck die Firma Keybase gekauft, um ihr Know-How im Bereich Encryption zu steigern. Nach eigenen Angaben wird sich Zoom noch weitere 45 Tagen mit allen Ingenieurskapazitäten weiter auf Datensicherheit konzentrieren.

Schritt 2: Abschluss eines Auftragsverarbeitervertrag (AVV) mit Zoom Inc., welcher von Zoom bereitgestellt wird.

Für eine rechtskonforme Nutzung muss eine Uni einen AVV mit Zoom Inc. schließen, welche diesen vorformuliert zur Verfügung stellt (abzurufen unter https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf, bei Vertragsschluss wird ein Exemplar inklusive der zu unterschreibenden Seiten übermittelt). Nach unserer Prüfung erfüllt der von Zoom Inc. angebotenen AVV die Mindestanforderungen, welche in Art. 28 DSGVO niedergelegt sind.

In unserer ersten Einschätzung sprachen wir davon, dass es noch besser sei, „einzelne Klauseln“ des AVV mit Zoom nachzuverhandeln. Diese Möglichkeit besteht nach unserem heutigen Kenntnisstand jedenfalls nicht ohne Weiteres. Wir halten eine Nachverhandlung indes auch nicht für nötig, da alle Vorgaben der DSGVO umgesetzt werden und dem Verantwortlichen in dem Vertrag umfassende Kontrollmöglichkeiten eingeräumt werden.

Verantwortliche, welche im Geltungsraum der EU sitzen, haben allerdings die Möglichkeit, neben dem AVV auch sog. Standard Contractual Clauses mit Zoom Inc. zu vereinbaren (Exhibit C unter

https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf). Dies ist unbedingt anzuraten, vgl. dazu noch Schritt 3. Vergleich zudem Schritt 10 für weiteres „Aktionspotential“, um als Verantwortlicher DSGVO-konform zu agieren.

Prüfung des AVV im Einzelnen:

Der AVV nimmt nicht ausdrücklich auf entsprechende Artikel der DSGVO Bezug. Es lassen sich jedoch alle zentralen Anforderungen einem entsprechenden Abschnitt im AVV zuordnen:

- Weisungsgebundenheit (Art. 28 Abs. 3 lit. a. DSGVO) in 3.2 AVV
- Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO) entsprechender Mitarbeiter bei Zoom in 4.2 AVV
- Einbeziehung von Art. 32 DSGVO (Art. 28 Abs. 3 lit. c DSGVO) in 6.2 AVV.
- Genehmigungspflicht für Unterauftragsverarbeiter und Weiterreichung der rechtl. Anforderungen „in der Kette“ (Art. 28 Abs. 3 lit. d DSGVO) in 5.2 AVV
    - Kritik: „Benachrichtigung“ nur durch Aktualisierung einer im Internet veröffentlichten Liste an „Subprocessors“ (= Unterauftragsverarbeiter). Der Verantwortliche muss selbst regelmäßig diese Liste überprüfen. Innerhalb von 10 Tagen könne der Verantwortliche der Unterauftragsverarbeitung widersprechen.
    - Rechtl. Bewertung: Hierin ist eine „allgemeine schriftliche Genehmigung“ des Verantwortlichen zu sehen iSd Art. 28 Abs. 2 S. 1 DSGVO. Fraglich ist, ob mit der Aktualisierung der Liste ohne Benachrichtigung des Verantwortlichen die Informationspflicht aus Art. 28 Abs. 2 S. 2 DSGVO erfüllt ist.

      (Eine explizite Information ist in den Standard Contractual Clauses vorgesehen. Auch deswegen sollten diese neben dem AVV vereinbart werden (siehe noch unten).)
- Pflicht zur Unterstützung des Verantwortlichen bei Erfüllung der Betroffenenrechten mit technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 lit. e DSGVO) in 8.2 AVV
- Bedingte Pflicht zur Unterstützung des Verantwortlichen bei Einhaltung der Art. 32-36 DSGVO (Sicherheit der Verarbeitung, Behördenmeldung bei Verstößen, Benachrichtigung des Betroffenen, Datenschutz-Folgenabschätzung) (Art. 28 Abs. 3 lit. f DSGVO) in 9.2 ff. AVV
- Löschung oder Rückgabe aller Daten nach Abschluss der Dienstleistungserbringung (Art. 28 Abs. 3 lit. g DSGVO) in 3.4 AVV
- Pflicht zur Informationsbereitstellung ggü. dem Verantwortlichen für behördliche Überprüfungen (Art. 28 Abs. 3 lit. h DSGVO) in 9.2 ff. AVV
- Genehmigungspflicht bei Einschaltung von Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO) in 5.2
- Pflicht dem Unterauftragsverarbeiter dieselben Pflichten aufzuerlegen, welche der Auftragsverarbeiter ggü. dem Verantwortlichen hat (Art. 28 Abs. 4 DSGVO) in 5.3, 5.4 AVV
- Schriftform oder elektronisches Format (Art. 28 Abs. 9 DSGVO)

Schritt 3: Abschluss der dem AVV angehängten Standard Contractual Clauses (SCC).

Aus folgenden Gründen sollten neben dem AVV auch die dem AVV angehängten SCCs unterzeichnet werden:

- Die auch bei Zoom anfallende unumgängliche Datenverarbeitung in den USA ist nach DSGVO derzeit noch in jedem Fall legal, da das sog. Privacy-Shield-Abkommen zwischen der EU und den USA noch in Kraft ist und Zoom Inc. insoweit zertifiziert ist.
  Bzgl. der Rechtmäßigkeit des Abkommens bestehen jedoch erhebliche Zweifel. Es ist ein
  Verfahren vor dem EuGH anhängig. Er wird wahrscheinlich im Laufe des Jahres 2020 entscheiden und Beobachter erwarten, dass er das Abkommen für ungültig erklärt.
  In diesem Fall käme der Vereinbarung sog. Standardvertragsklauseln i.S.d. Art. 46 Abs. 3 lit. a, 28 Abs. 6 DSGVO (Standard Contractual Clauses) mit Datenverarbeitern in den USA nicht mehr nur deklaratorische Wirkung, sondern konstitutive Wirkung zu. Nach einem entsprechenden Urteil wäre bei Abschluss des SCCs also zeitlich nahtlos ein Angebot von Zoom durch deutsche Hochschulen weiter möglich.

- Die SCCs nehmen konkreter als der AVV Bezug auf die Vorgaben der DSGVO und konkretisieren weiter die Pflichten von Zoom. Explizit anerkannt wird etwa auch die Geltung der DSGVO insgesamt, der Gerichtsstand des Verantwortlichen auch für Zoom, soweit eine Haftung von Zoom Inc. entsteht.

- Die SCCs räumen dem Verantwortlichen ggü. dem AVV weitergehende Rechte ein:

  - Recht, auch selbst einen Audit bei Zoom von einem unabhängigen Dritten durchführen zu lassen in Clause 5 (f)

  - Zoom ist verpflichtet, vor jeder neuen Unterauftragsverarbeitung die schriftliche Einwilligung einzuholen (statt nur genereller Aktualisierung der Liste), Clause 11.1

  - Recht, sich die teilweisen geschwärzten Kopien der Verträge von Zoom mit den Unterauftragsverarbeitern zuschicken zu lassen, Clause 5 (j)

Schritt 4: Implementierung der Software in das Hochschule-IT-System durch die Hochschule-IT und dabei Deaktivierung gewisser Funktionen und Programmstrukturen

Nahezu alle Einstellungen für Meetings können durch die Hochschule-IT global entweder als Default gesetzt, gesperrt oder ausgeschaltet (sie können dann wieder durch den Host aktiviert werden) werden. Es handelt sich insgesamt um mehr als hundert Optionen.

Die wesentlichen Einstellungen greifen unabhängig vom Client, mit dem am Meeting teilgenommen wird. Die Clients unterscheiden sich lediglich hinsichtlich der Funktionen für den Nutzer, die nicht überall gleichermaßen zur Verfügung stehen.

Bei Vornahme der Schritte 4 und 5 sollte die IT-Abteilung unbedingt mit dem/der Datenschutzbeauftragten zusammenarbeiten.

Gesperrt werden sollte etwa die Funktion Aufmerksamkeitstracking (nicht mehr relevant, da von Zoom bereits gesperrt) oder das hochschulweite Kontaktverzeichnis.

Schritt 5: Vornahme datensparsamer Voreinstellungen (defaults) durch die Uni-IT

vgl. Schritt 4

Beachten Sie den DSGVO-Grundsatz der Datenminimierung. Auch soweit gewisse datenintensivere Einstellungen für bestimmte (d.h. nicht bei allen) Lehrformate nötig sein sollten, deaktivieren Sie diese zunächst. Bei Bedarf kann der jeweilige Dozent die Einstellung wieder aktivieren (dies auch einmalig mit Speichern für alle seine zukünftigen Meetings).

Es ist auch immer vorzuziehen, dass TeilnehmerInnen selbst die Möglichkeit haben, in eine Datenverarbeitung (unabhängige etwaiger Rechtsgrundlagen z.B. der Interessenabwägung) nochmals tatsächlich individuell einzuwilligen bei Eintritt oder während des Meetings (zB. .Übertragung der Audio- und oder Videospur).

Schritt 6: Erstellung einer eigenen Datenschutzerklärung der Hochschule

Schritt 7: Erstellung von Anleitungen und Schulungsunterlagen für NutzerInnen zur datenschutzfreundlichen Nutzung von Zoom, etwa inkl. Sicherheitshinweise bzgl. Zoombombing, ggfs. in Zusammenarbeit mit anderen Hochschulen

Schritt 8: Ergänzung des Datenverarbeitungsverzeichnises gem. Art. 30 DSGVO um die Datenverarbeitungen in Zusammenhang mit Zoom

Schritt 9: Zusendenlassen der Verträge von Zoom mit Unterauftragsverarbeitern („Subprocessors“) und Anlage einer entsprechenden Liste, wozu der Verantwortliche gem. Clause 11.4 SCC verpflichtet ist

- Live schalten -

Schritt 10: Während des Betriebes
a) Monitoring der ggfs. neu hinzukommenden Unterauftragsverarbeiter
b) Anfordern und Durchsicht der jährlichen Datensicherheits-Auditierungen bei Zoom
c) ggf. Schulung der NutzerInnen zur datensicheren Nutzung von Zoom

Zu a)

Sofern die SCCs abgeschlossen wurden, ist Zoom verpflichtet, die schriftliche Genehmigung des Verantwortlichen bei Einschaltung weiterer Unterauftragsverarbeiter einzuholen. In diesem Fall sollte sich der Verantwortliche den entsprechenden Vertrag (teilweise geschwärzt) vorlegen lassen und prüfen, ob der Unterauftragsverarbeiter datenschutzrechtlich verantwortbar Aufgaben übernehmen kann. Bei „schwarzen Schafen“ sollte die Genehmigung versagt werden.
In diesem Fall muss Zoom gem. 5.2.1 AVV soweit möglich „reasonable alternatives“ anbieten. Nur

wenn solche nicht vorhanden sind, kann Zoom die Kündigung in Aussicht stellen. Dann kann der Verantwortliche noch einmal neu abwägen.

Zu b)

Gem. 9.4 AVV kann der Verantwortliche einmal im Jahr von Zoom Zertifizierungen und Audits verlangen, welche die Datensicherheit bei Zoom betreffen. Diese sollten angefordert werden und von einem kundigen Mitarbeiter der IT-Abteilung der Hochschule geprüft werden.

Literatur

- *Stoklas, Jonathan*, Datenschutz in Zeiten von Corona, ZD-Aktuell 2020, 07093; *John, Nicolas,* Corona is calling – Datenschutzrechtliche Probleme bei der Auswahl und Benutzung von Videokonferenzprogrammen für den Arbeits- und Hochschulalltag, DFN-Infobrief Sonderausgabe COVID19

- *Piltz, Carlo/Hessel, Stefan*, Berliner Datenschutzaufsicht: Stellungnahme und Checkliste zum Datenschutz bei Videokonferenzen, abzurufen unter https://www.reuschlaw.de/news/berliner-datenschutzaufsicht-stellungnahme-und-checkliste-zum-datenschutz-bei-videokonferenzen/; *Hansen-Oest, Stephan,* Hilfe…ist „Zoom" etwa eine Datenschleuder?, abzurufen unter https://www.datenschutz-guru.de/zoom-ist-keine-datenschleuder/#update16; *Berliner Datenschutzbeauftragte Maja Smoltczyk,* Zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, 08.04.20, abzurufen unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf; *Berliner Datenschutzbeauftragte Maja Smoltczyk,* Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen, 08.04.20, abzurufen unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf; Pressestelle des Landesbeauftragten für Datenschutz BaWü Stefan Brink, Datenschutzfreundliche technische Möglichkeiten der Kommunikation, 17.04.20, abzurufen unter https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/; Schröter, Nico/Zöllner, Lukas, Videokonferenz mit Zoom und Co.
  – Denn sie wollen wissen, was sie tun (dürfen), 15.04.2020, abzurufen unter https://www.lto.de/recht/hintergruende/h/datenschutz-behoerden-dsgvo-zoom-videokonferenz-unsicherheit/; *Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Dieter Kugelmann*, Einsatz von videogestützter Kommunikationstechnik zu Zwecken des Schulunterrichts während der Corona-Krise, abzurufen unter https://www.datenschutz.rlp.de/de/themenfelder-themen/videogestuetzte-kommunikationstechnik/ ; Prüfung verschiedener Dienste durch den Datenschutzbeauftragten des KantonsZürich,abzurufenunter https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/digitale-zusammenarbeit.html ; *Lukaß, Tom,* Videochats & Datenschutz – Heute: „Zoom", 6.04.20, letztes Update am 29.04.20, abzurufen unter https://www.datenschutz-notizen.de/videochats-datenschutz-heute-zoom-4325330/; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,* Datenschutz: Plötzlich Videokonferenzen – und nun?, abrufbar unter https://www.datenschutzzentrum.de/uploads/it/ULD-Ploetzlich-Videokonferenzen.pdf; *Schwenke, Thomas*, DSGVO-sicher? Videokonferenzen, Onlinemeetings und Webinare (mit Anbieterübersicht und Checkliste), 16.04.20, abrufbar unter https://datenschutz-generator.de/dsgvo-video-konferenzen-online-meeting/#Fazit

- Sydow/*Ingold*, Handkommentar Europäische Datenschutzgrundverordnung, 2. Aufl., Art. 28; Ehmann/Selmayr/*Bertermann*, Datenschutz-Grundverordnung, Art. 28; *Möllenkamp, Stefan/Ohrtmann, Jan-Peter,* Auftragsverarbeitung im Konflikt mit Beweissicherungsinteressen des Auftragnehmers, ZD 2019, 445; *Tausch, Karin/Tausch, Sebastian*, Datenschutz-Grundverordnung: So bekommen Sie die Auftragsverarbeitung in den Griff, BC 2018, 219; *Specht-Riemenschneider, Louisa/Schneider, Ruben,* Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, 503; *Gündel, Katharina,* Hauswarte und Handwerker – Auftragsverarbeiter im Sinne der DSGVO?, ZWE 2018, 429

- Sydow/*Mantz,* Art. 25 Rn. 12 ff.; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Art. 25, Art. 32; Kühling/Buchner/*Hartung* DSGVO Art. 25 Rn. 22; Gola/*Nolte/Werkmeister*, Art. 25 Rn. 21;

Taeger/Gabel/*Lang* Art. 25; Specht/Mantz/*Schneider,* Handbuch Europäisches und deutsches Datenschutzrecht, § 15; *Buss*, CR 2020, 1-6; Paal/Pauly/*Martini* Art. 32 Rn. 60