Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Behördlicher Datenschutzbeauftragter

Hinweise zur Nutzung von Konferenztools in der Lehre an der HWR Berlin während der Corona bedingten Einschränkungen

Aktualisiert: 15.4.2020

1. Allgemeines

Es ist damit zu rechnen, dass im Sommersemester 2020 Lehre an der HWR Berlin vollständig oder zu großen Teilen in Online-Formaten erfolgen muss. Im Zuge dessen erreichen den Datenschutzbeauftragten derzeit vermehrt Anfragen von den Lehrenden, welche Tools und Webanwendungen in der Online-Lehre datenschutzgerecht eingesetzt werden können. Hierzu möchten wir Ihnen einen Überblick über die hierzu bestehenden gesetzlichen Regelungen geben.

Der Datenschutz ist auch während der Corona-Situation nicht ausgehebelt und gilt vollumfänglich. Diese Hinweise sollen daher dazu beitragen, auch in der aktuellen schwierigen Lage die Datenschutzstandards einzuhalten.

2. Aktuelle Situation

Derzeit stehen die Konferenztools des Deutschen Forschungsnetzes nur eingeschränkt zur Verfügung, wobei natürlich auch hier mit stetiger Verbesserung zu rechnen ist. Aus Sicht der IT ist es daher für den regulären Betrieb erforderlich, neben den Konferenztools des DFN (Adobe Connect und Pexip) zusätzliche Dienste bereit zu stellen, die die eingeschränkte Verfügbarkeit des DFN kompensieren. Die Abteilung IT bereitet derzeit drei Systeme vor:

1. *Microsoft Teams* vorläufig[1] als extern gehostetes bzw. betriebenes System
2. *Big Blue Button* als dauerhaft intern gehostetes bzw. betriebenes System
3. *Jitsi* als dauerhaft intern gehostetes und betriebenes System

Ziel ist es hierbei mit Beginn der Lehre am 20. April 2020 neben den DFN Konferenztools drei funktionsfähige und stabile Systeme zur Verfügung zu stellen, die auch datenschutzrechtlich keine gravierenden Bedenken aufwerfen. Auf den Seiten des E-Learning-Zentrums und der IT der HWR Berlin wird fortlaufend über den Stand informiert, vermutlich jedoch erst ab KW 17.

Für die Einholung der informierten Einwilligung der Studierenden und Lehrenden zur Nutzung dieser intern administrierten Konferenztools werden zeitnah entsprechende Lösungen gefunden.

[1] Für einen längerfristigen / dauerhaften Betrieb über die Corona-Situation hinaus ist eine tiefergehende datenschutzrechtliche Prüfung erforderlich. Bei gleichzeitiger Nutzung mehrerer tausend Nutzer muss die Last des Datenstroms parallel laufender Online Veranstaltungen verteilt werden. Die interne IT-Infrastruktur reicht ggf. nicht aus. Aus diesem Grund soll *MS-Teams* die Infrastruktur extern ergänzen.

3. Nutzung externer Konferenztools für die Online-Lehre

Derzeit gibt es verständlicherweise Bestrebungen die vielfältig vorhandenen externen Konferenzsysteme in der Lehre zu nutzen. Naheliegende Kriterien für deren Wahl sind Funktionsfähigkeit und Geeignetheit. Es muss jedoch auch ein datenschutzkonformer Einsatz möglich sein und erfolgen. Ansonsten kann dies zu (meldepflichtigen) Datenschutzvorfällen führen. Grundsätzlich sind die Lehrenden für die datenschutzgerechte Gestaltung ihrer Lehre verantwortlich. Kommt es zu Datenschutzvorfällen, werden diese jedoch der HWR Berlin zugerechnet, da die Hochschule den Lehrbetrieb verantwortet. Um Datenschutzverstöße und die daraus resultierenden Folgen für Lehrende und Hochschule zu vermeiden, wird nachfolgend aufgezeigt, wie externe Tools datenschutzkonform eingesetzt werden können.

4. Empfehlung zur Nutzung von Konferenztools

Nutzen Sie vorrangig die von der HWR Berlin oder vom DFN administrierten und datenschutzrechtlich geprüften IT-Dienstleistungen, um Informationssicherheits- und Datenschutz-Risiken zu vermeiden.

Sollten Sie dennoch auf nicht durch die IT administrierte externe Tools ausweichen (müssen), beachten Sie bitte Folgendes:

Wenn personenbezogene Daten (vom Lehrenden oder Studierenden) durch das externe Tool bzw. einen externen Anbieter verarbeitet werden, so muss regelmäßig ein Vertrag zur Auftragsverarbeitung nach Artikel 28 DSGVO im Namen der Hochschule geschlossen werden. Dies wird mutmaßlich für nicht durch die IT administrierte Tools kaum möglich sein.

Ist die Zeichnung eines Vertrages zur Auftragsverarbeitung nicht möglich, dann achten Sie bitte darauf, dass

- es für nicht durch die IT administrierte Tools keinen Support von Seiten der IT gibt.
- ein Risiko darin besteht, dass Sie als Dozent ggfs. gemeinsam mit der HWR in die Haftung bezüglich der DSGVO geraten könnten.[2]
- durch die Verarbeitung Risiken für die Rechte und Freiheiten der Betroffenen entstehen können.
- die Datenverarbeitung (Serverstandort) vorzugsweise in Deutschland bzw. der EU vorgenommen wird. Wenn ein gleich geeigneter Anbieter innerhalb der EU operiert ist dessen Beauftragung regelmäßig verhältnismäßiger.
- so wenig wie möglich personenbezogene Daten von Ihnen und dem Studierenden verarbeitet werden. Bevorzugen Sie daher Tools, bei denen der Studierende kein eigenes Anmelde-Konto oder ein zu installierendes Clientprogramm benutzen muss. Die Nutzung des Webbrowsers ist empfehlenswerter, da man sich über die Browsereinstellungen und Add-Ons zu Cookies und Java-Skripten vor Werbetracking schützen kann.

[2] Lehrende nehmen zumindest faktischen Einfluss auf die Zwecke und Mittel der Datenverarbeitung durch den Drittanbieter. Dies ist insofern der Fall, da die HWR die Tools zum Zweck der Durchführung der Lehre nutzt. Hierdurch kann eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO entstehen. Der EuGH hat in den letzten Jahren einen sehr weiten Begriff der gemeinsam Verantwortlichen nach Art. 26 DSGVO geprägt (Stichwort "Facebook Fanpage"). Aus Art. 82 IV DSGVO folgt weiterhin, dass gemeinsam Verantwortliche grundsätzlich für den gesamten Schaden im Rahmen einer gemeinsamen Datenverarbeitung haften – also “quasi“ Gesamtschuldnerisch.

- möglichst keine Klarnamen zur Anmeldung oder im Stream verwendet werden und der Name, mit dem die Teilnahme am Meeting erfolgen soll, selbst festlegt werden kann. Eine Umsetzbarkeit der Empfehlung dürfte jedoch insb. vom Konferenzzweck, der Gruppengröße und dem Bekanntheitsgrad der Teilnehmer abhängen.
- mobile Apps des Anbieters keine Analyse-, Werbe- oder Trackingskripte im Hintergrund ausführen und ungefragt an Werbenetzwerke weiterleiten.
- ein geteilter Bildschirm nur zeigt, was für die Übertragung erforderlich bzw. notwendig ist.
- die Nutzung durch die Studierenden auf absolut freiwilliger Basis durchzuführen ist. Freiwillig bedeutet in diesem Zusammenhang, dass wenn jemand nicht über das Tool an der Lehrveranstaltung teilnehmen möchte oder kann, ihm dadurch keine Nachteile entstehen dürfen.
- es empfehlenswert ist, sich eine informierte Einwilligung der Studierenden für die Verarbeitung personenbezogener Daten einzuholen und diese zu dokumentieren.[3] Dies kann über eine Emailbestätigung erfolgen. Die Einwilligung muss jederzeit widerrufbar sein. Es ist anzunehmen, dass die Einwilligungen in Eigenregie eingeholt werden müssen, da die Fachbereichsverwaltungen ausgelastet sind. Eingeholte Einwilligungen müssen ggf. auf Anfrage der Aufsichtsbehörde nachgewiesen werden. Eine entsprechende Mustereinwilligung wird in den kommenden Tagen bereitgestellt.
- keine internen Dokumente der HWR Berlin oder personenbezogene Daten (wie Notenlisten, Anwesenheitslisten, etc.) geteilt oder anderweitig auf die Cloud-Server des externen Anbieters hochgeladen werden. Vorlesungsskripte fallen ggf. nicht darunter.
- Aufzeichnungen ebenfalls gesondert einwilligungsbedürftig sein können, wenn personenbezogene Daten verarbeitet werden. Zudem wird eine Aufzeichnung wohl stets den Ton umfassen und kann damit bei fehlender Zustimmung sogar wegen der Verletzung der Vertraulichkeit des Wortes nach § 201 Abs. 1 StGB strafbar sein.
- Chatverläufe im Anschluss an die Vorlesung gelöscht werden oder zumindest von der Einwilligung miterfasst werden.
- nichtöffentliche Vorlesungen unbedingt mit einem Passwort geschützt werden.
- wenn möglich eine implementierte Blurring-Funktion (ausgrauen des Hintergrundes) genutzt wird.

[3] Eine informierte Einwilligung (Informationspflichten Art. 13 DSGVO) umfasst insbesondere, welche personenbezogenen Daten zu welchen Zwecken durch den externen Anbieter verarbeitet werden , wie dessen Löschfristen aussehen, ob ggf. Dritte Zugriff auf die Daten haben und welche Datenschutz-Risiken bestehen (Werbe-Tracking auf Anmeldeseiten, Analyseskripte in der mobilen App, Auswertung des Nutzerverhaltens bei kostenlosen Tools, Zusammenführung der Analysedaten mit in der Vergangenheit erhobenen Analysedaten durch angebundene Werbenetzwerke, was zu breitem Profiling führen kann, etc.).

5. Bewertung externer Tools[4]

Sowohl von den Lehrenden als auch von der IT gingen viele Anfragen zur datenschutzrechtlichen Situation einzelner Konferenzsysteme ein. Die gängigen Systeme haben wir einer überblicksartigen Überprüfung unterzogen. Dabei wurden folgende Kategorien bewertet: Hostingmodell: (extern / intern), Lizenzmodell (Einzelplatz / Enterprise), Serverstandort, verarbeitete personenbezogene Daten, Möglichkeit zum Abschluss eines Vertrages zur Auftragsverarbeitung / Standardvertragsklauseln, Datenschutzerklärung, Informationssicherheit / TOMs, Datenübermittlung außerhalb EU / EWR, Tracking und Analyse auf der Anmeldeseite des Anbieters, sonstige Indikatoren.

Die obigen Kategorien wurden gewichtet und zu einer Gesamtbewertung aggregiert und in untenstehender Tabelle mit den Topbewertungsindikatoren aufgelistet.

Bewertungsmatrix

Empfehlenswert	Leichte Mängel im Datenschutz / IT-Sicherheit, aber immer noch empfehlenswert	Mittlere Mängel im Datenschutz / IT-Sicherheit, nur bedingt empfehlenswert	Erhebliche Mängel im Datenschutz / IT-Sicherheit, nicht empfehlenswert

Tool	Zoom	Skype	Jitsi	GotoMeeting	Cisco Webex	MS-Teams	Jitsi	Edudip next	Mikogo
Hostingvariante	Extern	Extern	Extern	Extern	Extern	Extern	Intern	Extern	Extern
Lizenzmodell	Einzelplatz / Enterprise	Einzelplatz	Einzelplatz	Einzelplatz / Enterprise	Einzelplatz / Enterprise	Enterprise	Open Source	Enterprise	Enterprise
Bewertung									
Begründung	Teils intransparente DSE und Abzüge bei privacy by default u. design / Aufmerksamkeitstracking / App sendet Daten an FB / teils Sicherheitslücken in Verschlüsselungsmethode / US CLOUD Act	Serverstandort global / genauer Standort unbekannt / Abzüge privacy by default / kein AV Vertrag möglich / US CLOUD Act	Serverstandort Unbekannt / keine DSE vorhanden / intransparente Datenverarbeitung	Keine Sicherheitszertifizierung / Übermittlung von Daten an Subunternehmer weltweit / US CLOUD Act	Abzüge privacy by default / Behält sich vor pbD an Unternehmen in den USA zu übermitteln / US CLOUD Act	2 MS-Accounts Host und Teilnehmer benötigen Office 365 / Teils intransparente DSE / Allgemeine Bedenken zur Praxis von MS beim Datenschutz bzw. zum datenschutzkonformen Betrieb von Office 365 / ggf. US CLOUD Act	Analyseskripte in IOS-App – **Bewertung Grün, wenn ohne IOS-App benutzt und unter Android aus dem Fdroid Store bezogen wird**	Keine Sicherheitszertifizierung / Teils intransparente DSE / externes Hosting / Server und Unternehmen in DT	Keine Sicherheitszertifizierung / Server in DT / externes Hosting / Sehr stark auf Datenschutz ausgelegt (USP)

Tool	Fast Viewer	Fast Viewer	Nextcloud Talk	BigBlueButton Enterprise
Hostingvariante	Extern	Intern	Intern	Intern
Lizenzmodell	Einzelplatz	Enterprise	Enterprise	Enterprise
Bewertung				
Begründung	Sicherheitszertifizierung für Bankensektor / vorhanden / externes Hosting	Sehr stark auf Datenschutz ausgelegt	Sehr stark auf Datenschutz ausgelegt	Starke Sicherheitsfeatures wie SSO, 2FA, Auth. über LDAP

Version	Datum	Dokumententyp	Autor	Änderung / Bemerkung	Klassifizierung
1.0	17.04.20	Merkblatt	Datenschutz	Release 1	Intern

[4] Stand 03/2020