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

Der behördliche Datenschutzbeauftragter

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

**Aktualisiert:** 20.04.2021

## 1. Allgemeines

Es ist damit auch weiterhin damit zu rechnen, dass die Lehre an der HWR Berlin vollständig oder zu großen Teilen in Online-Formaten erfolgen muss. Im Zuge dessen erreichen den Datenschutzbeauftragten Anfragen der Lehrenden, welche Tools und Webanwendungen in der Online-Lehre datenschutzgerecht eingesetzt werden können. Hierzu möchten wir Ihnen einen Überblick 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 Empfehlung

Aufgrund aktueller Empfehlungen der Aufsichtsbehörde können aktuell ausschließlich die intern gehosteten Videokonferenzsysteme empfohlen werden. Bei diesen handelt es sich um:

1. *Big Blue Button*
2. *Jitsi*

## 3. Nutzung externer Konferenztools für die Online-Lehre

Nach wie vor werden externe Konferenzsysteme in der Lehre an der HWR Berlin genutzt. Naheliegende Kriterien für deren Wahl sind Funktionsfähigkeit und Geeignetheit. Diese sind in der Praxis oft jedoch nicht rechtskonform einsetzbar. 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.

Nutzen Sie deswegen 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 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.[1]
- 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 zu bevorzugen.
- 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 Browsereinstellungen und Add-Ons vor Werbetracking schützen können.
- 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 unumgänglich ist, sich eine informierte Einwilligung der Studierenden für die Verarbeitung personenbezogener Daten einzuholen und diese zu dokumentieren.[2] 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 ist im Anhang.
- 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.

---

[1] 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.

[2] 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.).

- 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.

## Bewertung externer Tools[3]

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. Daneben floss die Empfehlung der Berliner Aufsichtsbehörde mit ein[4].

## Bewertungsmatrix

| | | | |
|---|---|---|---|
| Uneingeschränkt 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 | MS-Teams | DFN conf Pexip / Adobe Connect |
|---|---|---|---|---|---|---|---|---|
| **Hostingvariante** | Extern | Extern | Extern | Extern | Extern | Extern | Intern | Extern |
| **Lizenzmodell** | Einzelplatz / Enterprise | Einzelplatz | Einzelplatz | Einzelplatz / Enterprise | Einzelplatz / Enterprise | Enterprise | Enterprise | Enterprise |
| **Bewertung** | | | | | | | | |

| **Tool** | Jitsi | BigBlueButton |
|---|---|---|
| **Hostingvariante** | Intern | Intern |
| **Lizenzmodell** | Open Source | Enterprise |
| **Bewertung** | | |
| **Begründung** | | 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 |
| 1.1 | 28.04.2021 | Merkblatt | Datenschutz | Release 2 | Intern |

[3] Stand 04/2021
[4] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

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

Anhang A – Einwilligungserklärung Deutsch

# Hinweise zum Datenschutz für den Studierenden bei Nutzung externer Videokonferenzsoftware

Es ist damit zu rechnen, dass 2021 die Lehre an der HWR Berlin zu großen Teilen in Online-Formaten erfolgt. Mit diesem Merkblatt bekommen die Studierenden einen Überblick über das in der Lehrveranstaltung genutzte Programm und die datenschutzrechtliche Situation.

## 1. Externe / interne Tools

Die IT-Abteilung der HWR Berlin bietet zum Semesterstart drei intern administrierte Videokonferenzsysteme zur Durchführung der Lehre an. Diese sind einer Datenschutzprüfung unterzogen worden und bergen keine schwerwiegenden Mängel. Hierfür besitzt die HWR Hochschullizenzen.

In dieser Lehrveranstaltung soll jedoch ein nicht von der IT bzw. der Hochschule administriertes externes Videokonferenztool genutzt werden, das über eine Einzelplatzlizenz des Lehrenden beschafft wurde.

Diese Hinweise sollen Sie als Studierende, über die mit diesem Vorgehen bestehenden Risiken aufklären. Die Risiken unterscheiden sich von Tool zu Tool, weswegen hiermit ein allgemeiner Überblick gegeben werden soll. Eine detaillierte Bewertung einzelner Tools kann dem Merkblatt zur Nutzung von Konferenztools des behördlichen Datenschutzbeauftragten entnommen werden.

Daneben bekommen Sie als Student die unter Punkt 3 befindliche Einwilligung ausgehändigt. Die Einwilligung kann mit einer eindeutigen bestätigenden Handlung erfolgen. Zum Nachweis der Einwilligung und Vermeidung von Rechtsunsicherheiten, ist es empfehlenswert diese zu dokumentieren. Das Mittel ist grundsätzlich frei wählbar. Hierzu genügt z.B. eine Bestätigung per Mail oder einer Bestätigungsaufgabe in Moodle, nachdem dieser Informationstext dem Studierenden zur Verfügung gestellt wurde. Eine Unterschrift ist nicht zwingend notwendig, jedoch empfehlenswert.

## 2. Grundsätzliche Datenschutz-Risiken

Bei der Nutzung externer Konferenztools bestehen bestimmte Datenschutzrisiken, die folgend näher erläutert werden:

- Die datenverarbeitenden Server befinden sich oftmals im EU-Ausland. Dort gelten andere, oft niederwertigere Datenschutzbestimmungen, als sie die DSGVO hergibt. Für Übermittlungen ins Ausland bedarf es geeigneten Garantien bezüglich des vorgehaltenen Datenschutzniveaus. Diese wurden in der Vergangenheit regelmäßig mit Standardvertragsklauseln oder dem EU-US Privacy Shield begründet. Das Privacy Shield ist für ungültig erklärt worden, wonach eine Datenübermittlung in die USA derzeit nur schwierig möglich ist.
- Einzelplatzlizenzen bieten normalerweise nicht die fein granularen Einstellmöglichkeiten (privacy by default / privacy by design z.B. Übermittlung von Telemetriedaten) zum Datenschutz, wie sie Hochschullizenzen bieten.
- Verantwortlich für die Datenverarbeitung ist nicht die HWR Berlin, sondern der jeweilige Anbieter. Entsprechend können die Unternehmen die personenbezogenen Daten (auch die gesamten Text-, Ton-, Video- oder Bilddateien) für eigene Zwecke nutzen. Bei Hochschullizenzen ist dies i.d.R nicht möglich, da die Daten nur auf Weisung und für Zwecke der Hochschule vom Anbieter verarbeitet werden dürfen.

- Auf Anmeldeseiten für ein Nutzerkonto, Webanwendungen und mobilen Apps der Anbieter erfolgt regelmäßig eine Analyse des Nutzerverhaltens. Auf Anmeldeseiten laufen in Stichproben teils bis zu 40 Analyseskripte und 80 Cookies des Anbieters und angebundenen Werbenetzwerken. Diese Analyse-Daten werden für Marketing- und Werbezwecke ausgewertet und können zu einem umfassenden Profil Ihrer Persönlichkeit aggregiert und an externe Unternehmen weitergegeben werden.
- US-Unternehmen unterliegen dem US Cloud Act, welcher amerikanischen Behörden die Möglichkeit eröffnet auch dann auf gespeicherte Daten zuzugreifen, wenn die Speicherung außerhalb der Vereinigten Staaten von Amerika erfolgt.
- Die Anbieter nutzen normalerweise Unterauftragnehmer zur Erbringung der Leistung. Diese operieren aus Ländern wie China, Indien, Ägypten oder Mexiko. Die Unterauftragnehmer verarbeiten Ihre personenbezogenen Daten in diesen Ländern, wofür zur Übermittlung nach DSGVO ebenfalls geeignete Garantien für ein angemessenes Datenschutzniveau[5] erbracht werden müssten.
- Sicherheitsmaßnahmen (z.B. verschlüsselte Ende zu Ende Verbindungen, Sicherheitslücken in der Programmierung) entsprechen oft nicht dem aktuellen Stand der Technik
- Die Angebote der Anbieter bestehen zumeist aus Cloud-Anwendungen. Bei Datenverarbeitungen auf externen Cloudservern liegt die Hoheit über die Daten nicht bei der HWR Berlin. Manche Anbieter legen die Standorte und Länder der verarbeitenden Server nicht offen, sodass unklar ist, wo sich die Daten befinden und welchen Zugriffsmöglichkeiten diese ausgesetzt sind.
- Datenschutzerklärungen der Anbieter sind teilweise unvollständig und intransparent.
- Grundsätzliche besteht immer auch ein Risiko, dass sich die Anbieter nicht an geltende Datenschutz-Vorschriften halten und von abgegebenen Datenschutzversprechen abweichen.

## 3. Einwilligungserklärung

Ich willige in die Verarbeitung meiner personenbezogenen Daten im Rahmen der Onlinelehre durch das vom Lehrenden angebotenen Konferenztools für die Vorlesung XXXXXXX im Zeitraum xxxxxx ein. Ich habe die obigen Hinweise zum Datenschutz gelesen und bin mir der Datenschutz-Risiken bewusst.

Der Anbieter des Konferenztools verarbeitet hierbei in der Regel personenbezogene Daten der Datenkategorien:

Angaben zum Benutzer, Profildaten, Meeting-Metadaten, Authentifikationsdaten, Stream-Inhaltsdaten (Video-, Audio- und Textdateien), Diagnosedaten, Java-Skripte, Cookiedaten und Serverlogdaten.

Sobald ich die Webanwendung, die mobile App oder ein Clientprogramm des Anbieters aufrufe, ist der Anbieter für die Datenverarbeitung verantwortlich. Die Datenschutzerklärung des Anbieters kann ich hier einsehen.

Die Datenverarbeitung erfolgt ausschließlich zu folgenden Zwecken:

- Durchführung von Lehrveranstaltungen im Onlineformat unter Nutzung von Konferenz- und Streamingtools
- Abnahme von mündlichen Prüfungen
- Durchführung von Konferenzen, Online-Meetings, Videokonferenzen oder Webinaren

5 Art. 46 DSGVO

Diese Einwilligung erfolgt auf absolut freiwilliger Basis, d.h. wenn ich nicht einwillige, das jeweilige Konferenzsystem zu nutzen, dürfen mir dadurch keine Nachteile erwachsen. Der Lehrende muss mir die entsprechenden Inhalte auf andere Weise näherbringen.

Die Einwilligung kann ich jederzeit mit Wirkung für die Zukunft widerrufen. Dies kann ich unkompliziert per Email an den Lehrenden tun. Ab Zugang der Widerrufserklärung dürfen meine Daten nicht weiterverarbeitet werden. Sie sind unverzüglich zu löschen. Durch den Widerruf meiner Einwilligung wird die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung nicht berührt.

Die Betroffenenrechte, die mir aus der Datenverarbeitung des Konferenzsystemanbieters erwachsen (DSGVO Löschung, Sperrung, Berichtigung, etc.), mache ich gegenüber dessen Datenschutzbeauftragten geltend.

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

## Anhang B – Einwilligungserklärung Englisch

### Information on data privacy for the student when using external video conference software

It is to be expected that in 2021, teaching at the HWR Berlin will largely take place in online formats. This leaflet gives students an overview of the tool used in the course and the data protection situation.

### 1. External / internal tools

At the start of the semester, the IT department of the HWR Berlin will offer three internally administered video conferencing systems for teaching purposes. These systems have been subjected to a data protection audit and do not contain any serious deficiencies. The HWR has university licenses for these systems.

In this course, however, an external videoconferencing tool not administered by IT or the university is to be used, which was procured via a single-user license of the lecturer.

These notes are intended to inform you as a student about the risks involved in this procedure. The risks differ from tool to tool, so this is intended to provide a general overview. A detailed evaluation of individual tools can be found in the information sheet on the use of conference tools from the official data protection officer.

In addition, as a student you will be given the consent noted under point 3. The consent can be given with a clear confirmatory action. To prove the consent and to avoid legal uncertainties, it is recommended to document it by the lecturer. In principle, the means can be chosen freely. For example, a confirmation by e-mail or a confirmation task in Moodle is sufficient after this information text has been made available to the student. A signature is not absolutely necessary, but recommended.

### 2. Fundamental data protection risks

When using external conferencing tools, there are certain basic data protection risks, which are explained in more detail below:

- The data processing servers are often located in countries outside the EU, where different, often less stringent data protection regulations apply than those set out in the DSGVO. For transmissions abroad, suitable guarantees are required with regard to the level of data protection provided. In the past, these were regularly justified with standard contractual clauses or the EU-US Privacy Shield. The Privacy Shield has been declared invalid, making it difficult to transfer data to the USA at present.

- Single user licenses do not normally offer the finely granulated privacy settings (privacy by default / privacy by design, e.g. transmission of telemetry data) for data protection that university licenses offer.

- Responsible for data processing is not the HWR Berlin, but the respective provider. Accordingly, the companies may use the personal data (including all text, sound, video or image files) for their own purposes. In the case of university licenses, this is generally not possible, since the data either is processed by our own server or is only processed by the provider on the instructions and for the purposes of the university.

- An analysis of user behavior is regularly conducted on the registration pages for a user account, web applications and mobile apps of the providers. Random samples of up to 40 analysis scripts and 80 cookies from the provider and connected advertising networks are run on registration pages. This analysis data is evaluated for marketing and advertising purposes and can be aggregated into a comprehensive profile of your personality and passed on to external companies.

- US companies are subject to the US Cloud Act, which allows American Authorities to access stored data even if the storage takes place outside the United States of America.

- The providers usually use subcontractors to provide the service. These operate from countries such as China, India, Egypt or Mexico. The sub-contractors process your personal data in these countries, for which, in order to be transferred in accordance with the DSGVO, suitable guarantees for an adequate level of data protection would also have to be provided.

- Security measures (e.g. encrypted end-to-end connections, security gaps in the programming) often do not correspond to the current state of the art

- The providers' offerings mostly consist of cloud applications. In the case of data processing on external cloud servers, the sovereignty over the data does not lie with HWR Berlin. Some providers do not disclose the locations and countries of the processing servers, so it is unclear where the data is located and what access options it is exposed to.

- Data protection declarations of the providers are sometimes incomplete and intransparent.

- There is always a fundamental risk that the providers do not adhere to the applicable data protection regulations and deviate from the data protection promises made.

### 3. Consent of the student for processing personal data

I consent to the processing of my personal data within the scope of online teaching using the conference tool offered by the lecturer for the course XXXXX in the period xxxxxx. I have read the information mentioned above on data protection and i`m aware of the data protection risks.

The provider of the conference tool usually processes personal data of the data categories:

User details, profile data, meeting metadata, authentication data, stream content data (video, audio and text files), diagnostic data, Java scripts, cookie data and server log data.

As soon as I call up the web application, the mobile app or a client programme of the provider, the provider is responsible for the data processing. I can view the provider's privacy policy here LINK TO Privacy Statement oft he Provider

The data processing is exclusively for the following purposes:

- Holding courses in online format using conference and streaming tools

- Acceptance of oral examinations

- organisation of conferences, online meetings, video conferences or webinars

This consent is given on an absolutely voluntary basis, i.e. if I do not agree to use the respective conference system, I must not suffer any disadvantages as a result. The lecturer must introduce me to the relevant content in some other way. If i dont consent, i cant participate at

the conference. I am aware that the University Management does not agree with using external conference tools.

I can revoke this consent at any time with effect for the future. I can do this easily by email to the teacher. After receipt of the declaration of revocation, my data may not be processed further. They must be deleted immediately. Revoking my consent does not affect the legality of the processing that has taken place up to that point.

I assert the rights of the persons concerned, which arise for me from the data processing of the conference system provider (DSGVO deletion, blocking, correction, etc.), against the conference system provider's data protection officer.

---

Name, date, signature