h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Datenschutzleitfaden Home-Office, Videokonferenzen und Einsatz von Kommunikationstools

Prof. Dr. Thomas Wilmer, Datenschutzbeauftragter h_da

Stand 09.04.2020[1]

1. Grundregeln für den Einsatz von Tools

a. Auswahl: Reine Cloud Tools oder Lokale Installation?

Grundsätzlich sind die von der h_da lizenzierten Tools Adobe Connect und Zoom einzusetzen.

Für die eventuelle Auswahl von weiteren Tools gelten die folgenden Hinweise:

Bei der Toolprüfung sollte berücksichtigt werden, ob sich das Tool „komplett in der eigenen Hand befindet“, also lokal auf dem eigenen Server oder Rechner installiert wird, oder ob es sich um eine reine Cloud-Lösung handelt.

Zu bevorzugen sind lokal installierte Tools[2] oder Tools, welche von selbst ausgewählten Auftragsverarbeitern gehostet werden können. Hier ist weniger wahrscheinlich, dass Inhaltsdaten und Logdaten weitergegeben werden können[3].

Sollten ausnahmsweise andere Tools getestet oder benutzt werden, gelten die folgenden Hinweise[4]:

- Der Anbieter ist in der Regel als Auftragsverarbeiter nach Art. 28 DSGVO einzustufen und muss einen entsprechenden Auftragsverarbeitungsvertrag anbieten, der die technisch-organisatorischen Maßnahmen und das Datenschutzmanagement dokumentiert.

[1] Mit einem Update ist aufgrund zu erwartender weiterer Hinweise der hessischen Datenschutzaufsicht zu rechnen.
[2] Bei diesen muss selbstverständlich eine Klärung der Virenfreiheit und der Datensicherheit durch die IT erfolgen.
[3] Auch bei lokalem Hosting kann es sein, dass im betrieb Daten an den Anbieter übertragen werden. Die baden-württembergische Datenschutzaufsicht hat bei einer kursorischen Prüfung von lokal installierten Apps „Datenübertragungen festgestellt (…), bei denen Verantwortlicher, Zweck, Datenkategorien und Rechtsgrundlage unklar bleiben“, https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/
[4] Der Einsatz kann unter datenschutz@h-da.de mit mir abgestimmt werden.

- Der Toolanbieter darf keine Daten zu eigenen Zwecken (Big Data, Marketing) verwenden.
- Die Datenverarbeitung sollte möglichst in der EU stattfinden, dies gilt auch für Subunternehmer des Auftragsverarbeiters.
- Findet die Datenverarbeitung außerhalb der EU statt, muss durch geeignete Maßnahmen sichergestellt sein, dass das EU-Datenschutzniveau eingehalten wird (EU Standard Model Clauses, für die USA ist auch die Registrierung nach dem EU US Privacy Shield denkbar).

Bei der Nutzung von Cloud Tools sollte neben den unter b. folgenden Hinweisen vor allem darauf geachtet werden, dass Zugriffe des Tools auf eigene Kontakte oder sonstige lokale Daten sollten unterbunden werden. Last not least gilt, dass bei ausnahmsweiser Nutzung von nicht lizenzierten Tools aufgrund von Überlastung anderer Tools etc. (Sondernutzung „Corona Style“) geprüft wird, ob bei diesem anonymen Titel und Teilnehmerkennzeichnungen verwendet werden, soweit dies möglich ist. Je „riskanter“ das in Coronazeiten eingesetzte Tool ist (z.B. aufgrund einer Datenverarbeitung außerhalb der EU), umso stärker muss darauf geachtet werden, dass möglichst wenig personenbezogene Daten verarbeitet werden.

b. Datenschutzfreundlicher Einsatz von Tools

Grundsätzlich sind möglichst wenig personenbezogene Daten bei der Toolnutzung zu übertragen und zu erfassen. Zugleich sollte darauf geachtet werden, dass auch sonstige vertrauliche Informationen geschützt bleiben.

aa. Generelle Toolnutzung

Aus Datenschutzgründen ist im Einzelnen zu empfehlen,

- dass geprüft wird, ob der Audioeinsatz genügt oder Videoübertragung erforderlich ist,

- dass Aufzeichnungsfunktionen deaktiviert sind,

- dass allen Teilnehmenden bekannt ist, wer im Call ist oder mithören kann[5],

- dass Protokolldaten zur Teilnahme nur bei Vorliegen einer Rechtsgrundlage aktiviert sind (etwa bei zulässigen Teilnahmeverpflichtungen),

- dass möglichst wenig Namen genannt werden,

- dass Text-Chats über datenschutzfreundliche und Ende-zu-Ende-verschlüsselte Plattformen stattfinden,

[5] Das unbefugte Abhörens oder Aufzeichnen des nichtöffentlich gesprochenen Wortes ist strafbar nach § 201 StGB

- dass keine Geschäftsgeheimnisse oder sensiblen Daten[6] über das Tool übertragen werden, etwa dass in Videokonferenzen nicht unnötig über Sozialdaten oder Gesundheitsdaten Einzelner gesprochen wird,

- dass vor Bildschirmfreigaben nicht alle nicht benötigten Programme geschlossen werden, um versehentliche Einblendungen etwa von Posteingängen zu verhindern,

- verhindert wird, dass Social Media Applikationen geöffnet / aktiv sind, welche auf Daten aus der Toolnutzung zugreifen können,

- gespeicherte Daten umgehend gelöscht werden, sobald sie nicht mehr benötigt werden; dies gilt insbesondere für private Kontaktdaten.

bb. Nutzung im Home-Office

Hier sollte darauf geachtet werden,

- ob die Daten überhaupt im Home Office verarbeitet werden dürfen (z.B. weil in einem Forschungsprojekt keine Freigabe der Datenverarbeitung außerhalb der Hochschule vorgesehen ist),

- dass der Datenverkehr über geschützte Netze läuft,

- Dritte nicht unnötig mithören können, insbesondere bei sensiblen Daten,

- dass nur Geräte mit Passwortschutz eingesetzt werden,

- dass soweit möglich Daten auf dem Server des Arbeitgebers und nicht lokal gespeichert werden,

- bei lokaler Speicherung ein Passwortschutz erfolgt,

- bei sensiblen Daten sollte keine ungenehmigte Anbindung des privaten Geräts an Speicherclouds oder Ähnliches bestehen, welche einen Datenzugriff erlauben könnten,

- und Vorgaben vorhandener Richtlinien der h_da eingehalten werden.

Hinzuweisen ist im Übrigen auf die Tipps für sicheres mobiles Arbeiten des Bundesamtes für Sicherheit in der Informationstechnik[7].

[6] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 I DSGVO)

[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf

2. Überblick über andere (als die lizenzierten) Tools

Bei der aufgeführten – nicht abschließenden - Liste ist zu beachten, dass je nach Tool der Einsatz auch von der Nutzung datenschutzfreundlicher Einstellungsmöglichkeiten oder lokaler Installation abhängen kann. Soweit keine personenbezogenen oder vertraulichen Daten übertragen werden, kann im Einzelfall auch ein „unsichereres“ Tool eingesetzt werden. Die bereits freigegebenen Tools Adobe Connect und ZOOM sind hier nicht zusätzlich ausgeführt (siehe zu ZOOM Hinweise unter 3 e.bb..))

Video- und Audiotools und Tools zur Datenteilung[8]	Datenhaltung nur in der EU[9]	Keine Datensammlung zu eigenen Zwecken	Hinweise zur DSGVO-Compliance	Open Source basiert?	Links	Gesamt-beurteilung[10]
Confluence			Eigenes Hosting in EU möglich		https://www.atlassian.com/de/trust/privacy/gdpr#data-transfers	
Gotomeeting					https://www.logmeininc.com/de/gdpr/gdpr-compliance https://www.logmeininc.com/de/legal/privacy-shield	
Jitsii			Lokal installierbar		https://jitsi.org/news/security/ https://jitsi.org/meet-jit-si-privacy/	
Matrix			https://www.golem.de/news/messenger-matrix-org-server-gehackt-1904-140655.html		https://matrix.org/	
Nextcloud Talk			Lokal installierbar		https://nextcloud.com/de/gdpr/	
Rocketchat			Lokal installierbar		https://rocket.chat/gdpr	
Skype			Datenauswertung ungeklärt		https://support.skype.com/de/skype/all/privacy-security/	
Whatsapp			Datenauswertung ungeklärt, insb. Weitergabe an facebook		https://faq.whatsapp.com/de/iphone/28041111/	

3. Materialsammlung mit weiteren Hinweisen

[8] Siehe auch technologische Übersicht bei https://en.wikipedia.org/wiki/Comparison_of_web_conferencing_software

[9] Ein roter oder Eintrag bedeutet nicht, dass die Datenübertragung außerhalb der EU nicht den Art. 44ff. DSGVO entspricht, sondern lediglich, dass eine solche wahrscheinlich (gelb) oder sicher (rot) stattfinden kann.

[10] GRÜN: Einsatz unbedenklich
GELB: Einsatz abhängig von der Beachtung besonderer Datenschutzmaßnahmen
ROT: Einsatz möglichst nur vorübergehend und unter VermFeidung der Offenbarung sensibler Daten

a. Datenschutzaufsichten

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit:

Telearbeit und Mobiles Arbeiten. Ein Datenschutz Wegweiser. Stand: Januar 2019
https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit[11]

Informationen zum digitalen Lernen und der digitalen Kommunikation zur Unterstützung hessischer Schulen im Zeichen der Covid-19-Pandemie

https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/informationen-zum-digitalen-lernen-und-der-digitalen

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Datenschutzfreundliche technische Möglichkeiten der Kommunikation

Stand 27.03.2020
https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie

https://www.datenschutz-bayern.de/corona/sonderinfo.html

Der Landesbeauftragte für den Datenschutz Niedersachsen

Informationen zum mobilen Arbeiten durch öffentliche Stellen (entspricht den bayrischen Hinweisen)

https://lfd.niedersachsen.de/startseite/allgemein/mobiles-arbeiten-corona-186918.html

[11] Hier sind in Kürze weitere Hinweise zu erwarten, Hinweise für Hochschulen sind abrufbar unter https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein

Plötzlich im Homeoffice - und der Datenschutz? Die Landesbeauftragte für Datenschutz Schleswig-Holstein informiert
https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Einsatz von videogestützter Kommunikationstechnik zu Zwecken des Schulunterrichts während der Corona-Krise
https://www.datenschutz.rlp.de/de/themenfelder-themen/videogestuetzte-kommunikationstechnik/

Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Empfehlungen für KMU zur Verarbeitung personenbezogener Daten in Heimarbeit
https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/Homeoffice_bei_KMU.pdf

b. Hessisches Kultusministerium

Handreichung für Lehrkräfte zum Umgang mit Sozialen Netzwerken in hessischen Schulen

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Handreichung%20Soziale%20Netzwerke%20-%20Stand%20Februar%202015.pdf

c. Bundesamt für Sicherheit in der Informationstechnik

Tipps für sicheres mobiles Arbeiten Stand 28.3.2020

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf

d. European Union Agency for Cybersecurity (ENISA)

Top Tips for Cybersecurity when Working Remotely“Artikel der European Union Agency for Cybersecurity (ENISA)
Stand: März 2020
https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely

e. Datenschutzinformationen zu einzelnen Tools

aa. Skype

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) stellt fest: Bericht über angebliche Untersagung des Schulunterrichts per Skype durch den HmbBfDI ist eine Falschmeldung
https://datenschutz-hamburg.de/pressemitteilungen/2020/03/2020-03-26-falschmeldung-skype

bb. Zoom

Zoom und Datenschutz, Informationspapier von Prof. Dr. Alexander Roßnagel / Chief Information Officer der Universität Kassel vom 03.04.2020
(Hinweis: Laut Presseinformationen ist ZOOM aktuell dabei, Datenschutzherausforderungen weiter anzugehen)
https://www.uni-kassel.de/einrichtung/index.php?eID=dumpFile&t=f&f=1092&token=0568e4e5bd9f740baf69bf375411bb6c8bd2e37a