WEBINARE, ONLINE-MEETINGS & CO

Europa, wir haben ein Problem

In unserer Juni-Ausgabe haben wir im Artikel »Online reden und lernen« darauf hingewiesen, dass für Organisationen innerhalb der EU die Nutzung von z. B. Zoom problematisch ist. Seitdem ist viel passiert. Mittlerweile ist klar: Sie ist in fast allen Fällen illegal. Dieser Artikel erläutert im ersten Teil ganz detailliert, warum das so ist. Er versucht aber auch, Lösungen und Alternativen aufzuzeigen.

AM 6. AUGUST 2020 unterzeichnete Donald Trump ein Dekret, das nach Ablauf einer 45-Tagesfrist (20. September) den Einsatz von und Geschäftsverbindungen mit den (zum Teil) chinesischen Handy-Apps TikTok und WeChat in den USA verbietet. Die Begründung: Von diesen Apps gingen signifikante Bedrohungen aus, sie seien chinesische Spionageinstrumente. Die Amerikaner wissen genau, worum es dabei geht, denn in ihren Funktionen und Datensammeleigenschaften ähneln die beiden chinesischen Apps den amerikanischen Apps Snapchat, Instagram, facebook und WhatsApp. Mittels Auslesens der Daten dieser (Handy-)Programme ist es den US-Behörden möglich, z. B. europäische User zu überwachen – und das passiert auch. Und zwar in einem Ausmaß, wie es die US-amerikanische Politik offensichtlich keinesfalls mit den Daten von US-Bürgern durch ausländische Behörden geschehen lassen will.

Und Europa? Europäische Politik und Wirtschaft sind von amerikanischer Software in einem ungesunden Ausmaß abhängig, als Folge gibt es kaum politischen Widerstand gegen die Überwachung europäischer Bürger durch US-Unternehmen und -Behörden – politischen Widerstand nicht, rechtlichen jedoch schon. Daher ist die Nutzung vieler amerikanischer Programme und Dienste durch europäische Unternehmen streng genommen verboten – bzw. nur unter ganz bestimmten Voraussetzungen erlaubt. Am 16. Juli 2020 stellte der Europäische Gerichtshof in seinem Urteil fest, dass der »Privacy Shield«, unter dem die Datenübertragung in die USA zulässig war, nicht mehr gilt. Damit wurden die Voraussetzungen für den Einsatz amerikanischer Software weiter verschärft. Welche Konsequenzen hat dieses Urteil? Ab wann gilt es? Was bedeutet das konkret für Unternehmen, Trainingsinstitute, Anbieter von Online-Seminaren, Personalabteilungen?

EuGH Urteil vom 16. Juli 2020

Unmittelbar nach Veröffentlichung des Urteils durch den EuGH wurden von verschiedensten Organisationen und Medien offensichtlich schon länger vorbereitete Interpretationen des Urteils kommuniziert. Diese Interpretationen sind stark vom Interesse der jeweiligen Kommunikatoren geprägt und widersprechen einander zum Teil. Während einerseits aufgezeigt wird, dass die Übertragung personenbezogener Daten in die USA nicht mehr zulässig sei, weil der Privacy Shield für ungültig erklärt wurde, wird andererseits behauptet, dass diese Datenübertragung sehr wohl zulässig sei, dann nämlich, wenn sie auf Basis sogenannter Standardvertragsklauseln passiert. Diese Klauseln habe der EuGH nämlich explizit als zulässig bezeichnet. Was stimmt also?

Erfreulicherweise muss man sich in dieser Sache nicht auf die Interpretationen anderer ver-

lassen. Man kann alles selbst im Urteil nachlesen. (Der Link zum Urteil steht im Info-Kasten rechts unten.) Am Ende des Urteils, ab Randnummer 199, steht Folgendes:

»199 Daraus folgt, dass Art. 1 des DSS-Beschlusses [Anm.: = Datenschutzschild-Beschluss, bekannt als »Privacy Shield«] *mit Art. 45 Abs. 1 der DSGVO, ausgelegt im Licht der Art. 7, 8 und 47 der Charta, unvereinbar und somit ungültig ist.*

200 Da Art. 1 des DSS-Beschlusses untrennbar mit dessen Art. 2 bis 6 sowie dessen Anhängen verbunden ist, führt seine Ungültigkeit zur Ungültigkeit des gesamten Beschlusses.

201 Nach alledem ist festzustellen, dass der DSS-Beschluss [Anm.: = Privacy Shield] *ungültig ist.«*

Und zusammenfassend in Randzahl 203:

»[...] 5. Der Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes ist ungültig.«

Der Privacy Shield, von der EU-Kommission nach der Aufhebung von »Safe Harbour« im Jahr 2015 mit den Amerikanern ausverhandelt, gilt also nicht mehr. Wer bisher personenbezogene Daten auf Basis des Privacy Shield in die USA transferiert hat (oder transferieren lassen hat), darf das nicht mehr tun.

Wie sieht es nun mit den Standardvertragsklauseln aus? Im Urteil steht unter Randnummer 203:

»[...] 4. Die Prüfung des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern [...] anhand der Art. 7, 8 und 47 der Charta der Grundrechte hat nichts ergeben, was seine Gültigkeit berühren könnte. [...]«

Die Standardvertragsklauseln gelten also nach wie vor und können auch in Zukunft für den Transfer personenbezogener Daten in Drittstaaten genutzt werden.

Wer aber aufgrund dieses Absatzes im Urteil behauptet, damit sei der Datentransfer in die USA auf Basis von Standardvertragsklauseln zulässig, der hat entweder nicht das gesamte Urteil gelesen oder verschweigt ganz bewusst Wesentliches. Denn: Das gilt nur, wenn der betreffende Drittstaat für die Daten der EU-Bürger ein Datenschutzniveau bietet, das jenem der EU gleichwertig ist. Und das schließt die USA in fast allen Fällen aus. All das steht im Urteil, zum Teil in Randnummer 203:

»[...] 2. Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der Verordnung 2016/679 sind dahin auszulegen, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen, dass die Rechte der Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein Schutzniveau genießen, das dem in der Europäischen Union durch diese Verordnung im Licht der Charta der Grundrechte der Europäischen Union garantierten Niveau der Sache nach gleichwertig ist. [...]«

Und das gilt auch nur dann, wenn die Standardvertragsklauseln im Einzelfall von der Organisation (z. B. Unternehmen), die den Datentransfer verantwortet, geprüft werden:

»134 [...] Folglich obliegt es vor allem diesem Verantwortlichen bzw. seinem Auftragsverarbeiter, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren.«

Dass in den USA kein gleichwertiger Datenschutz besteht, findet sich im Urteil an mehreren Stellen, z. B. in den Randnummern 180 bis 185.

»180 Demzufolge lässt Section 702 des FISA in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung von Überwachungsprogrammen [...] Einschränkungen bestehen. Genauso wenig ist erkennbar, dass für [...] Nicht-US-Personen Garantien existieren. Unter diesen Umständen ist diese Vorschrift [...] nicht geeignet, ein Schutzniveau zu gewährleisten, das dem durch die Charta [...] garantierten Niveau der Sache nach gleichwertig ist.«

Das hat viel mit dem Foreign Intelligence Surveillance Act (FISA) zu tun, einem US-amerikanischen Gesetz, das alle amerikanischen Anbieter von Kommunikationsdiensten dazu verpflichtet, die Daten ausländischer Bürger zu sammeln, zu speichern und den Behörden zur Verfügung zu stellen. Diese Dienste müssen dem Gesetz Folge leisten, unabhängig davon,

Vereinfacht zusammengefasst hat der Datenschutzaktivist Max Schrems die Verletzung der Rechte europäischer Bürger durch amerikanischen Unternehmen und Behörden bis zum EuGH gebracht.
Die von ihm gegründete Datenschutz-Non-Profit-Organisation noyb.eu gibt auf ihrer Website viel Hintergrund-Info zum EuGH Urteil und auch wertvolle Tipps für Unternehmen, welche Schritte nach dem Urteil getan werden könnten und sollten: www.noyb.eu/de

Info

Links zum EuGH Urteil vom 16. Juli 2020
Link, der direkt zum Urteil in deutscher Sprache weiterleitet:
www.magazintraining.com/eugh
der komplette Original-Link:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=15266299
Alternativ führt auch Folgendes zum Urteil: in einer Suchmaschine »C-311/18« eingeben und dann auf der ersten Ergebnisseite das Dokument auf Deutsch öffnen.

was sie in Verträgen mit europäischen Unternehmen vereinbaren.

Zusammenfassung, mögliche Lösungen

Die Datenübertragung in Drittstaaten auf Basis von Standardvertragsklauseln ist nur dann erlaubt, wenn im Drittstaat das gleiche Datenschutzniveau wie in der EU gewährleistet ist.

Auch wenn es viele gerne anders hätten und auch darstellen: Das EuGH Urteil vom 16. Juli untersagt den Transfer personenbezogener Daten in die USA nicht nur auf Basis des Privacy Shield, sondern auch auf Basis von Standardvertragsklauseln, außer wenn zusätzliche Maßnahmen getroffen werden, die das gleiche Datenschutzniveau wie in der EU gewährleisten, was im Einzelfall ziemlich schwierig sein wird. Die Überprüfung der Einzelfälle obliegt laut EuGH neben den Daten-Verantwortlichen und den Auftragsverarbeitern auch den nationalen Datenschutzbehörden, die die Einhaltung der Datenschutzregeln überwachen sollen.
Es gibt dazu auch Stellungnahmen von Behörden, die das bestätigen (siehe Links im Info-Kasten auf Seite 14). Die österreichische Datenschutzbehörde verweist auf ihrer Website auf die Stellungnahme des Europäischen Datenschutzausschusses und fasst ganz kurz zusammen, dass eine Berufung auf Standardvertragsklauseln nur möglich sei, wenn zusätzliche Sicherheitsgarantien einbezogen werden. Die Berliner Datenschutzbeauftragte fordert als Konsequenz des EuGH Urteils dazu auf, »in den USA gespeicherte personenbezogene Daten nach Europa zu verlagern.« In der Tat scheint das auf lange Sicht der einzige verlässliche Weg zu sein, nicht mit dem Gesetz in Konflikt zu geraten.
Den meisten Lösungswegen stehen nämlich Hindernisse entgegen. Ein Beispiel: Microsoft und andere amerikanische Großkonzerne, für die in dieser Sache sehr viel auf dem Spiel steht, haben schon vor einigen Jahren damit begonnen, in Europa Datencenter (Serverfarmen) zu errichten, damit die Daten europäischer Bürger nicht mehr in die USA transferiert werden. Diese Lösung wurde aber von der amerikanischen Regierung (bzw. dem Gesetzgeber) 2018 zunichte gemacht, als der CLOUD Act erlassen wurde, ein Gesetz, das amerikanische Unternehmen dazu verpflichtet, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewähren, wenn die Speicherung nicht in den USA erfolgt.

Hier geht es um ein Grundrecht europäischer Bürger, das von den USA konsequent und völlig bewusst verletzt wird. Nun könnten wir Europäer unsere Grundrechte ändern. Das wird eher nicht passieren. Oder es könnten die Amerikaner ihre Gesetze (FISA, CLOUD Act) ändern. Auch das ist höchst unwahrscheinlich. Es scheint wirklich darauf hinauszulaufen, dass in Europa europäische Software- und Internetlösungen entwickelt und genutzt werden müssen. Was aus heutiger Sicht wie ein Projekt unvorstellbaren Ausmaßes wirkt, kann man auch als große Chance für Europa, seine Eigenständigkeit und seine Wirtschaft sehen. Wenn es zu keiner Beilegung dieses Grundrecht-Konflikts kommt, müssen in Zukunft alle Lösungen aus europäischer Hand kommen, in Europa Kompetenzen aufgebaut, Serverfarmen errichtet, Infrastruktur geschaffen werden.
Davon betroffen sind sogar Produkte wie Microsoft Office und das Betriebssystem Windows. Der europäische Datenschutzbeauftragte hat im Juli einen 29-seitigen Bericht (Link im Info-Kasten auf Seite 14) veröffentlicht, in dem er u. a. fünf konkrete Punkte darlegt, in denen Microsoft gegen die Grundrechte der EU-Bürger verstößt. In dem Bericht werden europäische Behörden dazu aufgerufen, ihren Einsatz von Microsoft-Produkten zu überdenken. Das ist auch für europäische Unternehmen höchst interessant, denn für sie gilt selbstverständlich dasselbe Recht.
Die Auswirkungen des EuGH Urteils sind von solch gigantischer Tragweite, dass in Österreich zunächst das Typische passiert ist, nämlich nichts – oder fast nichts. Adobe, Amazon (AWS), Apple, Cisco, Cloudflare, Dropbox, Facebook, Google, Microsoft, Salesforce, Zoom – wer kann das heute wie ersetzen? Apropos heute: Die Auswirkungen des EuGH Urteils gelten seit Erlassung, also seit 16. Juli 2020. Eine Übergangs- oder Schonfrist gibt es nicht.

Abgesehen von den beschriebenen Standardvertragsklauseln und »Binding Corporate Rules« (für die dieselben Einschränkungen gelten) sowie Sonderfällen wie Hotelbuchungen gibt es zwei Möglichkeiten, personenbezogene Daten in die USA zu übermitteln, ohne dabei die Rechte der betroffenen Personen zu verletzen: Verschlüsselung und Einwilligung.

Verschlüsselung

Wenn die Daten ausschließlich verschlüsselt übermittelt werden und die Datenverarbeiter und -empfänger keine Möglichkeit der Entschlüsselung haben, dann ist eine Übermittlung in einen Drittstaat DSGVO-konform. Das Problem daran: Viele der Funktionen der Anbieter stehen dann nicht mehr zur Verfügung. Meist sind da auch jene Funktionen dabei, deretwegen man überhaupt die Leistungen dieser Anbieter in Anspruch nimmt. Für eine Cloud-Speicherung (z. B. ein Back-up) der Daten, den Austausch von Daten in einer Gruppe und alle verwandten Dienste kann das aber sehr wohl sinnvoll sein. Mit Verschlüsselung kann man sogar Dienste wie Dropbox nutzbar machen, die sonst ein

Datenschutz-Fiasko sind. Ein Beispiel für einen Open-Source-Verschlüsselungsdienst, der auch mit Dropbox kompatibel ist: cryptomator.org. Oder man nutzt eine Dropbox-Alternative, die von Vornherein mit Verschlüsselung arbeitet und sicher ist: crypt.ee oder securesafe.com (beide kostenpflichtig, es gibt auch einige weitere). Größere Unternehmen werden ohnedies ihre eigenen Server betreiben bzw. Serverspace anmieten und verwalten. Damit ist es dann möglich, z. B. einen eigenen Nextcloud-Server zu betreiben. Das ist ein mächtiges Instrument, das schnell eingerichtet ist und es erlaubt, Groupware-Anwendungen laufen zu lassen, Dateien gemeinsam zu bearbeiten, Kalender einzurichten und miteinander zu teilen, miteinander zu chatten und vieles mehr. Und das alles am Server der eigenen Wahl, also garantiert ohne Datentransfer in ein Drittland. Nextcloud ist Open Source, läuft auf allen gängigen Desktop- und Handy-Betriebssystemen und bietet auch Ende-zu-Ende-Verschlüsselung. Für die Einrichtung gibt es fertige Installations-Skripte, die Miete für ausreichend Serverspace (je nach Personenanzahl) beginnt bei österreichischen Anbietern bei ca. 10,– € pro Monat, für kleine Unternehmen je nach Anforderungen bei 20,– bis 50,– € pro Monat.

Einwilligung zum Datentransfer

Von allen betroffenen Personen für den Datentransfer in einen Drittstaat eine Einwilligung einzuholen, ist nur für ganz kleine Organisationen möglich. Ein gutes Beispiel dafür wären Vorstandsmitglieder eines Vereins, die eine Online-Besprechung durchführen. Diese Vorstände können sich dann auch in einem Zoom-Call treffen, ohne in Probleme mit dem Datenschutz zu geraten, das Einverständnis aller Personen vorausgesetzt. Für größere Organisationen ist das mit der Einwilligung kein gangbarer Weg: Erstens ist die Einholung einer Einwilligung häufig nicht praktikabel und – im Fall von Beschäftigten oder auch Studierenden – einem Unwirksamkeitsrisiko wegen mangelnder Freiwilligkeit ausgesetzt. Und zweitens kann sie jederzeit von jeder Person ohne Angabe von Gründen zurückgenommen werden. Dann müsste die Datenanwendung sofort gestoppt werden, zumindest für die Daten dieser Person.

Software für Videokonferenzen

Was die DSGVO betrifft, unterscheiden sich Videokonferenzen nicht von anderen Datenverarbeitungen. Die Daten-Verantwortlichen und Auftragsverarbeiter müssen sicherstellen, dass die personenbezogenen Daten vor dem Zugriff anderer geschützt werden. Da nach dem EuGH Urteil Privacy Shield und Standardvertragsklauseln als rechtliche Basis einer Datenübertragung in die USA in der Regel wegfallen, bleiben nur wenige Optionen:

1. Die Daten nicht an amerikanische Dienstleister übertragen.
2. Die Daten verschlüsseln.
3. Eine gültige Einwilligung aller betroffenen Personen einholen.
4. Auf geltendes EU-Recht pfeifen.

Das Problem mit dem ersten Punkt: Die populärsten Anbieter sind alle amerikanisch: Adobe Connect, Cisco WebEx, Google Meet, Microsoft Teams, Skype, Zoom. In einem Bericht (Link: siehe Info-Kasten auf Seite 14) der bereits zitierten Berliner Datenschutz-Beauftragten vom 2. Juli, also noch vor dem EuGH Urteil, werden Anbieter von Videokonferenz-Diensten hinsichtlich der Einhaltung der DSGVO bewertet. Dabei kommt ein einfaches Ampelsystem zur Anwendung: Grün markiert sind Anbieter, bei denen keine Mängel gefunden wurden. Gelb markiert sind Anbieter mit Mängeln, die eine rechtskonforme Nutzung des Dienstes zwar ausschließen, deren Beseitigung allerdings vermutlich ohne wesentliche Anpassungen der Geschäftsabläufe und der Technik möglich ist. Rot markiert sind Anbieter, bei denen Mängel vorliegen, die eine rechtskonforme Nutzung des Dienstes ausschließen und deren Beseitigung vermutlich nicht oder nur sehr schwer möglich sind. Hier ist auszugsweise eine Kopie des Dokuments:

Cisco WebEx	https://www.webex.com/de
Google Meet	https://apps.google.com/meet/
Microsoft Teams	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software
Skype	https://www.skype.com/de/
Zoom	https://zoom.us

Na bumm. Wir brauchen also eine andere Lösung. Das Problem mit Punkt 2 (Verschlüsselung) ist erstens, dass eine Verschlüsselung nur möglich ist, wenn sie vom Dienstleister auch angeboten wird und zweitens, dass eine Verschlüsselung aller Videostreams extrem ressourcenhungrig ist und bereits ab einer nicht sehr großen Teilnehmerzahl die Serverkapazitäten und auch die Bandbreite der einzelnen

Teilnehmer sprengt. Unter anderem deswegen wird eine echte Ende-zu-Ende-Verschlüsselung aller Streams nicht angeboten.
Die Schwierigkeiten mit Punkt 3 (Einwilligung) sind bereits weiter oben (Seite 13) genau beschrieben. Für größere Unternehmen, Trainingsinstitute mit externen Teilnehmern, Universitäten und Fachhochschulen ist das Einholen einer Einwilligung aller Teilnehmer nicht praktikabel bzw. unter Umständen ungültig (keine echte Freiwilligkeit).
Bleibt Punkt 4: Pfeif auf den Datenschutz, interessiert eh niemanden! Genau das wird tatsächlich praktiziert: von Unternehmen, Fachhochschulen, Trainern, Schulen, Vortragenden und vielen mehr. Aber wollen wir das? Wollen wir als Personalabteilung einen externen Trainer engagieren, dem die Rechte unserer Mitarbeiter egal sind? Wollen wir als Schule die Rechte der uns anvertrauten Kinder missachten? Als Fachhochschule die Studierenden zu einer nicht rechtmäßigen Einwilligung zwingen? Wollen wir das wirklich, als Gesellschaft? Vor allem: Es geht hier nicht um irgendwelche Rechte, es geht um von der Verfassung garantierte, persönliche Grundrechte.

Wollen wir als Personalabteilung einen externen Trainer engagieren, dem die Rechte unserer Mitarbeiter egal sind?

Wenn einem das alles egal ist, hat man in Österreich – zumindest vorläufig noch – die Möglichkeit, das Recht zu brechen, ohne größere Konsequenzen befürchten zu müssen, indem man sich von den amerikanischen Dienstleistern in Auftragsverarbeitungsverträgen und sonstigen über die Standardvertragsklauseln hinausgehenden Vereinbarungen bestätigen lässt, dass keine personenbezogenen Daten weitergegeben werden, auch wenn das nicht stimmt. Diese Verträge kann man dann im Fall des Falles der Datenschutzbehörde vorlegen und sich unwissend stellen. Was dann passiert, ist reine Spekulation. Aber es sieht so aus, als ob man mit dieser Methode bis auf Weiteres einer Strafe entgehen könnte. Diesen Weg scheinen aktuell viele österreichische Unternehmen einzuschlagen. Abermals muss die Frage erlaubt sein: Wollen wir das? Recht brechen und sich dumm stellen?

Zum Glück gibt es in der Bewertung der Berliner Datenschutz-Beauftragten auch einige Anbieter, für die die Ampel auf Grün steht:

- Netways (nws.netways.de/de/apps/jitsi/)
- sichere-videokonferenz.de
- Tixeo Cloud (www.tixeo.com)
- Werk21 (www.werk21.de)
- Wire (www.wire.com/de)

Bei diesen Anbietern gibt es also keine rechtlichen Probleme. Aber es gibt durchaus Probleme technischer oder anderer Natur. Netways und sichere-videokonferenz basieren auf der Open-Source-Lösung Jitsi (jitsi.org). Jitsi hat einige Nachteile gegenüber Anbietern wie Zoom: So sind u. a. die Moderations-Funktionen deutlich eingeschränkt, es sind alle Personen in der Videokonferenz quasi gleichberechtigt. Das ist für ein Vorstandsmeeting oder eine kleine Gruppenbesprechung in Ordnung, für Online-Unterricht, Online-Seminare usw. eignet es sich aber nicht. Außerdem haben wir in der Redaktion noch kein Jitsi-Meeting ohne Bandbreiten-Probleme erlebt. Das heißt aber nichts über diese beiden Anbieter, man müsste sie testen, vielleicht bieten sie ja völlig ausreichende Server-Kapazitäten. sichere-videokonferenz.de ist (vorläufig) ohnedies ein Gratis-Angebot, das kann man nach Belieben testen und nutzen. Ein paar Klicks genügen und schon ist eine Videokonferenz erstellt, sind Teilnehmer eingeladen und los geht's. Netways bietet 30 Tage lang einen Gratis-Zugang an, danach kostet das Angebot je nach maximaler Teilnehmeranzahl in einem Meeting 40,– oder 250,– € pro Monat.
Beim Anbieter Wire sind laut Angaben auf der Website die Videokonferenzen auf bis zu 4 Teilnehmern ausgerichtet, das schließt viele Anwendungsfälle aus.
Tixeo Cloud bietet Videokonferenzen für deutlich mehr Teilnehmer an, das hat allerdings seinen Preis: Für »ab 20 Teilnehmer« kostet das Angebot 2.880,– € pro Jahr. Für »ab 50 Teilnehmer« sind es dann schon 9.000,– €.
Bleibt Werk21, das auf der Open-Source-Software BigBlueButton (bigbluebutton.org) basiert. Diese ist vom Funktionsumfang ver-

Info

Stellungnahme der Berliner Datenschutz-Beauftragten
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf

FAQ der europäischen Datenschutzbehörde (auf Englisch)
https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

Website der österreichischen Datenschutzbehörde
https://www.dsb.gv.at/internationaler-datenverkehr

Bericht des europäischen Datenschutzbeauftragten zur Nutzung von Microsoft
https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf

Hinweise der Berliner Datenschutz-Beauftragten zu Anbietern von Videokonferenz-Diensten
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

gleichbar mit Zoom. Als Moderator kann man Teilnehmer stumm schalten, aus dem Meeting entfernen, ihnen unterschiedliche Rollen zuweisen. Man kann Break-out-Rooms anlegen, die Teilnehmer also in mehreren Kleingruppen gleichzeitig arbeiten lassen. Es können vorbereitete Präsentationen abgespielt werden. Man kann den eigenen Bildschirm freigeben, Videokonferenzen aufzeichnen usw. Mit BigBlueButton lässt sich auch als Lehrer oder Trainer arbeiten. Es ist aber sehr ressourcenhungrig, vor allem ab einer gewissen Teilnehmeranzahl. Im Prinzip ist es ja Open Source, man kann es sich also herunterladen und auf dem eigenen Server installieren. Allerdings ist das alles andere als trivial. Mit einem Server ist es nämlich nicht getan. Für eine optimale Performance muss man auch einen STUN- und einen TURN-Server einrichten und es bedarf starker Server mit einer sehr schnellen und stabilen Internet-Anbindung. Da braucht man erstens Experten für Einrichtung und Wartung und zweitens kostet das einiges an Geld. Für große Unternehmen oder Universitäten mit eigener IT-Abteilung und Inhouse-Servern ist das eine hervorragende Möglichkeit, ziemlich sicher die beste Lösung am Markt. Für kleinere Unternehmen, Trainer, Vortragende usw. gibt es Anbieter wie Werk21, die einem das alles abnehmen. Weitere Anbieter, die dem europäischen Recht entsprechen und in Deutschland die Server betreiben, sind (die Liste ist nicht vollständig):
meeting.levigo.cloud/b (Gratis-Angebot)
senfcall.de (Gratis-Angebot)
collocall.de, bbbserver.de, rackspeed.de, owncube.de, blueboxs.de
Die Preise variieren stark, auch innerhalb der verschiedenen Pakete eines Anbieters, je nach dem, auf wie viele Teilnehmer es ausgerichtet sein soll und ob man einen eigenen Server (dezidiert) oder nur einen geteilten (shared) erhält. Das fängt bei 7,– € pro Monat an und geht bis zu 315,– €. Die Gratis-Angebote sind für den professionellen Einsatz eher nicht gedacht.

Der österreichische Anbieter fairkom.eu hat ein beeindruckendes Angebot. In seinen »Pro-Paketen« (small um 12,– bis large um 69,– € pro Monat) ist sowohl das auf Jitsi basierende fairmeeting als auch das auf BigBlueButton basierende fairteaching inkludiert. Aktuell stehen alle Funktionen auch kostenlos zur Verfügung. Wer sie professionell nutzt, soll aber ein der Teilnehmerzahl entsprechendes Paket buchen. Eine Empfehlung von unserer Redaktion ist das aber noch nicht. Dazu müssten wir die Funktionen noch ausgiebig testen. Genau das haben wir vor, auch mit einigen der anderen erwähnten Anbietern. Den Testbericht gibt es in der nächsten Ausgabe. □