Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Maja Smoltczyk

2735 G

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin

An die
Vorsitzende des Hauptausschusses
im Abgeordnetenhaus von Berlin
Frau Franziska Becker

Niederkirchnerstraße 5
10117 Berlin

Datum: 23. September 2020
GeschäftsZ.: 659.13.7

Berichtsauftrag aus der 77. Sitzung des Hauptausschusses vom 26. August 2020

Sehr geehrte Frau Becker,

im Nachgang zu der o. g. Sitzung des Hauptausschusses übersende ich Ihnen anliegend die gewünschte Einschätzung. Ich möchte Sie bitten, diese auch den übrigen Mitgliedern des Ausschusses zur Verfügung zu stellen.

Für Rückfragen stehe ich selbstverständlich gern zur Verfügung.

Mit freundlichen Grüßen

M. Smoltczyk

Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Maja Smoltczyk

Telefon: 030 13889-0
E-Mail: mailbox@datenschutz-berlin.de

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Friedrichstr. 219
10969 Berlin
Besuchereingang:
Puttkamer Str. 16-18

Telefon: (030) 13889-0
Telefax: (030) 215 50 50
mailbox@datenschutz-berlin.de

Sprechzeiten

tgl. 10-15 Uhr, Do. 10-18 Uhr
(oder nach Vereinbarung)

Erreichbarkeit

U6: Kochstr.
Bus: M29, 248

Internet

https://datenschutz-berlin.de

Das Beschlussprotokoll der 77. Sitzung des Hauptausschusses am 26. August 2020 enthält zu TOP 58 folgenden Auftrag:

„Weiter wird die Berliner Beauftragte für Datenschutz und Informationsfreiheit, möglichst zum 23.9.2020, um eine Einschätzung zur Notwendigkeit von Datenschutz und IT-Sicherheit im Bereich Digitalisierung und Schule gebeten."

Aktuelle Ausgangslage

Angesichts steigender Infektionszahlen besteht eine berechtigte Sorge, wie die Schulen vor dem Hintergrund einer bevorstehenden zweiten Infektionswelle für den Fall möglicher Schulschließungen aufgestellt sind, um Schülerinnen und Schüler im Homeschooling zu unterrichten. Die an meine Behörde gerichteten Anfragen und Beratungsersuchen zeigen auf der einen Seite, dass Schulleitungen und Lehrkräfte vielfach verunsichert und auch überfordert sind, die Entscheidung zu treffen, welche digitalen Werkzeuge datenschutzgerecht im Unterricht eingesetzt werden dürfen. Viele wünschen sich Orientierung. Auf der anderen Seite beschweren sich Eltern darüber, dass Schulen Softwareprodukte einsetzen, deren Datenschutzkonformität zweifelhaft ist und suchen unsere Hilfe, um deren Einsatz in den Schulen zu unterbinden.

Besondere Datenschutzanforderungen im Schulkontext

Wann immer personenbezogene Daten verarbeitet werden, muss dies unter Berücksichtigung des Datenschutzes geschehen. Im schulischen Kontext spielt das Thema Datenschutz eine extrem wichtige Rolle. Die Datenschutz-Grundverordnung (DS-GVO) stellt Kinder und Jugendliche unter einen besonderen Schutz. Erwägungsgrund 38 zur DS-GVO führt insoweit aus, Kinder verdienten bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Der besondere Schutz soll sich insbesondere auf die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen richten.

Datenschutzgerechte Schul-Digitalisierung

Gerade im Kontext der Digitalisierung an Schulen stellt sich eine Reihe datenschutzrechtlicher Fragen. Der Einsatz digitaler Lernmittel birgt Gefahren für die Persönlichkeitsrechte der Schülerinnen und Schüler, aber auch der Lehrkräfte. Im Schulkontext werden sensible Daten der Kinder und Jugendlichen verarbeitet, deren wirksamer Schutz ein selbstverständliches Anliegen sein sollte. Es muss zum einen die Rechtmäßigkeit der Verarbeitung der Daten sichergestellt werden, zum anderen sind ausreichende technische Schutzvorkehrungen zu treffen, um zu gewährleisten, dass auch die Anforderungen an die Datensicherheit eingehalten werden.

Leider wird meine Behörde von der Senatsverwaltung für Bildung nur sehr unzureichend in diesen notwendigen Prozess der datenschutzgerechten Ausgestaltung einbezogen. Im Gegenteil: Selbst das aktive Zugehen auf die Senatsverwaltung z. B. in Bezug auf den Lernraum bereits im Februar 2020 hat erst nach wiederholter Erinnerung unsererseits dazu geführt, dass erstmalig im August 2020 ein erstes persönliches Gespräch zwischen der Senatsverwaltung für Bildung und meiner Behörde stattgefunden hat. Um Datenschutzbelange überhaupt angemessen berücksichtigen zu können, bedarf es hier erheblicher Verbesserungen in der Kommunikation.

Handlungsbedarf aus Datenschutzsicht

Die im Land Berlin geltenden Rechtsvorschriften des Schulgesetzes und der aus dem Jahre 1994 stammenden Schuldatenverordnung enthalten überhaupt keine Regelungen zum Einsatz digitaler Werkzeuge. In der Praxis bedeutet dies, dass ein Einsatz von digitalen Lernmitteln und Lernplattformen in den Schulen nur rechtmäßig erfolgen kann, wenn die Eltern bzw. Schülerinnen und Schüler hierfür ihre freiwillige und informierte Einwilligung erteilt haben. Da zwischen den Schulen und den Schülerinnen und Schülern ein Sonderrechtsverhältnis besteht und damit für eine Freiwilligkeit in diesem Kontext wenig Raum besteht, ist es notwendig, zügig die entsprechenden Rechtsgrundlagen zu schaffen, um hier für alle Beteiligten die notwendige Rechtssicherheit zu erreichen.

Außerdem halten wir es für notwendig, dass die Senatsverwaltung für Bildung Rahmenbedingungen für die Schulen und Lehrkräfte für den Einsatz digitaler Werkzeuge in rechtlicher und technischer Hinsicht definiert und meine Behörde hierbei einbezieht. Auf dieser Grundlage müssten Angebote eingeholt werden, die dann auf ihre pädagogische Eignung sowie datenschutzgerechte Ausgestaltung geprüft werden müssen. Es wird dringend empfohlen, dass die Senatsverwaltung für Bildung klare Vorgaben definiert, welche digitalen Lernmittel von den Schulen genutzt werden können. So können den Lehrkräften rechtssichere Angebote unterbreitet werden.

In technischer Hinsicht muss dabei von vornherein ein besonderes Augenmerk auf den Einsatz datenschutzgerechter Angebote gerichtet werden. Es kann nicht hingenommen werden, dass Daten in einer Weise gespeichert werden, die Missbrauch, Nutzung der Daten für Werbezwecke oder Erstellung von Nutzungsprofilen ermöglicht. Nur so kann auch bei allen Beteiligten das notwendige Vertrauen in Bezug auf die digitalen Angebote aufgebaut werden.

Bei der Einführung von technischen Systemen, unabhängig davon, ob es um die Einführung oder Weiterentwicklung von Fachverfahren, die Nutzung digitaler Lernplattformen oder die Beschaffung von Endgeräten für die administrative oder die edukative Nutzung geht, muss meine Behörde einbezogen werden. Da eine Nutzung ohne Einhaltung der durch den Datenschutz gestellten Anforderungen rechtswidrig ist, besteht sonst die große Gefahr, dass Investitionen in Technologien oder Produkte getätigt werden, die später nicht eingesetzt werden dürfen.

Bei der Entwicklung der im Schulbereich eingesetzten Fachverfahren ist es zwingend notwendig, dass diese bereits in der Konzeptionsphase im Hinblick auf Datenschutzanforderungen geprüft und gegebenenfalls entsprechend angepasst werden. Eine frühzeitige Einbeziehung meiner Behörde kann verhindern, dass Gelder in Verfahren oder Komponenten investiert

werden, die später nicht datenschutzkonform eingesetzt werden können und dann entweder unter hohem Aufwand angepasst oder gar ersetzt werden müssen. Von besonderer Wichtigkeit ist eine Bewertung nach Gesichtspunkten des Datenschutzes und der IT-Sicherheit immer dann, wenn Schnittstellen zum Austausch personenbezogener Daten zwischen mehreren Systemen geschaffen werden sollen.

Auch bei der Beschaffung digitaler Endgeräte für Lehrkräfte oder Schülerinnen und Schüler muss der Datenschutz bereits bei der Definition der Anforderungen mitgedacht werden. Für den edukativen Bereich beschaffte Endgeräte müssen beispielsweise ohne einen Cloudzugang bei Anbietern außerhalb der Europäischen Union nutzbar sein. Außerdem wäre es sinnvoll, Systeme zu bevorzugen, die eine einfache Trennung verschiedener Nutzungsarten ermöglichen. Folglich haben aus Perspektive des Datenschutzes mobile Computer wie Laptops deutliche Vorteile gegenüber Tablets, da diese z. B. über einen sog. Bootstick in einer vollständig von der normalen Umgebung getrennten Umgebung gestartet werden können. Eine Vermischung von administrativen und edukativen Daten im Falle der Lehrkräfte oder aber privaten und edukativen Daten im Falle der Schülerinnen und Schüler wäre so weitgehend ausgeschlossen. Hinzu kommt, dass Laptops auch weitere Vorteile gegenüber Tablets haben, sobald die Nutzung über den Konsum von Medienangeboten hinausgeht. Selbst wenn bei vielen Tablets eine zusätzliche Tastatur beschafft werden kann, ist dies doch immer mit weiteren Kosten verbunden, während eine solche bei Laptops notwendig vorhanden ist.

Kurzfristig umsetzbare Empfehlungen

Abschließend möchte ich darauf hinweisen, dass es mir insbesondere vor dem Hintergrund möglicherweise notwendiger Schulschließungen ein wichtiges Anliegen ist, praxisgerechte Hinweise zu geben, wie die datenschutzgerechte Nutzung digitaler Angebote zur Aufrechterhaltung des Unterrichtsbetriebes möglich sein kann. Bereits kurz nach den Schulschließungen im Frühjahr dieses Jahres hat meine Behörde *„Hinweise zum datenschutzkonformen Einsatz von digitalen Lernplattformen durch Schulen"* entwickelt, um den Schulleitungen und den Lehrkräften Kriterien an die Hand zu geben, anhand derer eine Auswahl datenschutzgerechter Produkte für die Unterrichtsgestaltung erkannt und ausgewählt werden konnten. Auch hat meine Behörde in den vergangenen Monaten Kurzprüfungen der Videokonferenz-Dienste verschiedener Anbieter vorgenommen und *„Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten"* veröffentlicht. Beide Dokumente sind diesem Schreiben als Anlagen beigefügt.

Darüberhinausgehend halte ich die im Folgenden skizzierten konkreten Maßnahmen im Hinblick auf die Gefahr einer bevorstehenden zweiten Infektionswelle kurzfristig und mit vertretbarem Aufwand für umsetzbar:

- Ein datensicherer Messengerdienst sollte eingerichtet werden. Dies ist auch heute schon möglich. Das Kultusministerium Baden-Württemberg hat beispielsweise Threema Work Education für alle Lehrkräfte und Schülerinnen und Schüler zur Verfügung gestellt. Wünschenswert ist perspektivisch sicher die Einführung einer durch das Land Berlin selbst betriebenen Lösung. Allerdings könnte die Nutzung von Threema Work Education kurzfristig ein datenschutzgerechter Kompromiss sein.

- Die Senatsverwaltung für Bildung sollte kurzfristig ein datenschutzkonformes Videokonferenzsystem auf Basis verschiedener Open Source Programme wie Nextcloud Talk, Jitsi Meet oder Big Blue Button für die Schulen zur Verfügung stellen.

- Bei der Beschaffung von digitalen Endgeräten für Lehrkräfte und Schülerinnen und Schüler sollte die Wahl auf Laptops fallen, da diese wesentlich vielseitiger einsetzbar sind als Tablets. Außerdem bieten sie mehr Freiheiten bei der Softwareauswahl und sind auch ohne Nutzerzugang bei Dienstleistern flexibel nutzbar. Nicht zuletzt könnten sie durch günstigere Preise u. U. auch umfassender an die Schülerinnen und Schüler verteilt werden, womit auch eine einheitliche Lernumgebung für alle gegeben wäre.

Anlagen

Hinweise zum datenschutzkonformen Einsatz von digitalen Lernplattformen durch Schulen

Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit als Datenschutz-Aufsichtsbehörde wird vor dem Hintergrund der Corona-Pandemie verstärkt hinsichtlich des datenschutzkonformen Einsatzes von Videokonferenzlösungen kontaktiert. Um unserer Aufsicht unterliegenden Verantwortlichen die Prüfung der Rechtmäßigkeit der Nutzung verschiedener Lösungen zu erleichtern, veröffentlichen wir folgend die Ergebnisse der durch uns durchgeführten Kurzprüfungen der Videokonferenz-Dienste verschiedener Anbieter, wobei wir den Schwerpunkt auf die Bewertung der Rechtskonformität der von den Anbietern angebotenen Auftragsverarbeitungsverträge gelegt haben.

Sofern die Anbieter nach einer Kurzprüfung rechtskonforme Auftragsverarbeitungsverträge bereithalten sowie uns Informationen bzw. einen Test-Zugang zur Verfügung gestellt haben, erfolgte zudem eine kursorische Untersuchung einiger technischer Aspekte der Dienste. Die Ergebnisse dieser Untersuchungen haben wir in den Anmerkungen zu den einzelnen Anbietern zusammengefasst, um es den Verantwortlichen zu erleichtern, einen für ihre Zwecke geeigneten Dienst auszuwählen und, soweit erforderlich, ergänzende technische und organisatorische Maßnahmen zu ergreifen. Zu diesen Maßnahmen kann es insbesondere gehören, sich der Identität der Teilnehmenden der Konferenz und der Sicherheit der Verbindung zu versichern, wenn der gewählte Dienst hierfür nur Mechanismen bereithält, die in Anbetracht der Sensitivität der zu besprechenden Daten nicht angemessen sind. Leider sind nach derzeitigem Entwicklungsstand alle betrachteten Dienste mit Ausnahme von Wire in der Standardkonfiguration für den Austausch von Informationen mit hohem Schutzbedarf nicht geeignet. Weitere nützliche Hinweise zur datenschutzgerechten Konfiguration und Nutzung von Videokonferenzdiensten, die wir hier nicht wiederholen, sind den vielfältigen Veröffentlichungen zu entnehmen, die in jüngster Zeit zu dem Thema erschienen sind.

Die vorliegende Bewertung erstreckt sich ausschließlich auf Dienste, die Videokonferenzen als Software-as-a-Service (SaaS) anbieten. Aus technischer Sicht ist jedoch diesen Angeboten mit vorkonfigurierten Einstellungen, die in vielen Fällen auch nicht verändert werden können, der Betrieb eines Dienstes durch die Verantwortlichen selbst (ggf. auf einer durch einen Auftragsverarbeiter bereitgestellten Plattform) vorzuziehen, da sie dann die Umstände der Verarbeitung vollumfänglich selbst bestimmen können. In Abhängigkeit von Umständen und Risikolage kann dies ggf. auch die einzig verfügbare rechtskonforme Lösung sein. Bei Software-as-a-Service (SaaS) sollten Lösungen bevorzugt werden, bei denen die Verantwortlichen möglichst viele Rechte haben, um die verwendete Lösung an ihre Anforderungen anzupassen.

Auch wenn unsere rechtliche Analyse keine Mängel aufgedeckt hat, bedeutet dies nicht, dass diese nicht vorliegen und entbindet Verantwortliche nicht von ihren gesetzlichen Pflichten. Es wird ausdrücklich darauf hingewiesen, dass keine umfassende Prüfung der Angebote erfolgte, insbesondere keine umfassende technische Prüfung und in der Regel auch keine Prüfung der Datenschutzerklärungen. Letztere betreffen lediglich die eigenverantwortlichen Datenverarbeitungen der Videokonferenzsystem-Anbieter. Nicht von den Datenschutzerklärungen umfasst sind diejenigen Datenverarbeitungen, die verantwortliche Stellen mit Sitz in Berlin durchführen, wenn sie die Dienste in Anspruch nehmen. Wir empfehlen insbesondere ergänzend eine Prüfung der Datenschutzerklärungen und technischer Aspekte sowie der Frage, ob die Anbieter sich möglicherweise entgegen dem Auftragsverarbeitungsvertrag die Verarbeitung der Nutzungsdaten zu eigenen Zwecken oder Zwecken Dritter vorbehalten oder eine solche vornehmen. Soweit rechtliche Mängel in den geprüften Dokumenten vorhanden sind, dürfen die Dienste nur genutzt werden, wenn abweichende Vereinbarungen mit den Anbietern getroffen wurden.

Grün markiert sind Anbieter, bei denen wir bei unserer Kurzprüfung keine Mängel gefunden haben. In der rechtlichen Prüfung gelb markiert sind Anbieter, bei denen wir Mängel gefunden haben, die eine rechtskonforme Nutzung des Dienstes zwar ausschließen, deren Beseitigung allerdings vermutlich ohne wesentliche Anpassungen der Geschäftsabläufe und der Technik möglich ist. In der technischen Prüfung bedeutet eine gelbe Markierung, dass die Anbieter derzeit (nur) unter Beachtung bestimmter Rahmenbedingungen nutzbar sind. Rot markiert sind Anbieter, bei denen Mängel vorliegen, die eine rechtskonforme Nutzung des Dienstes ausschließen und deren Beseitigung vermutlich wesentliche Anpassungen der Geschäftsabläufe und/oder der Technik erfordern, etwa wenn nach dem Vertrag die Anbieter Auftragsdaten auch zu eigenen Zwecken verarbeiten, der Vertrag Datenlöschungen nur verspätet oder eingeschränkt vorsieht oder die Anforderungen an die Einbindung von Subunternehmern derzeit nicht ausreichend ausgestaltet sind und voraussichtlich Änderungen in den Verträgen zwischen Anbietern und Subunternehmern erforderlich sind.

Die Liste wird laufend ergänzt, wenn im Rahmen unserer Aufsichts- und Beratungstätigkeit weitere Angebote geprüft wurden. Wir ermuntern zudem ausdrücklich Anbieter, die ihre Videokonferenzlösungen Berliner Verantwortlichen anbieten möchten, uns über ihr Angebot zu informieren und uns die Vertragsdokumente und einen Test-Zugang zur Verfügung zu stellen. Wir regen an, vor einer Einreichung selbstkritisch zu prüfen oder durch die/den betriebliche/n Datenschutzbeauftragte/n oder Angehörige der rechtsberatenden Berufe prüfen zu lassen, ob die Verträge den gesetzlichen Anforderungen entsprechen. Hierzu empfehlen wir auch die Lektüre der Anmerkungen zu den bereits geprüften Verträgen sowie unserer „Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten“, die Sie unter https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/corona-Pandemie.html finden. Diese kann Verantwortlichen auch die Prüfung der Verträge von Anbietern, die bisher nicht in der Liste enthalten sind, erleichtern.

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

R*	T†	Dienst	URL	Version der Dokumente	Rechtliche Mängel bzgl. Auftragsverarbeitung	Ort der Verarbeitung nach Vertrag auf EU/EWR beschränkt
		Blizz	https://www.blizz.com/de/	Blizz Auftragsverarbeitungsvertrag (https://www.blizz.com/de/auftragsverarbeitungsvertrag/), Endnutzer-Lizenzvereinbarung – Blizz (https://www.blizz.com/de/eula/), jeweils ohne Datum, letzter Abruf 28.5.2020 [Deutsch]	ja, siehe Anmerkung Anbieter hat Änderungen angekündigt	nein
		Cisco WebEx	https://www.webex.com/de	Universelle Cloud-Vereinbarung Version 9.3 vom 15.4.2020 [Deutsch]; Master Data Protection Agreement, December 2019 [Englisch]; Digital River Ireland Ltd. Allgemeine Geschäftsbedingungen und Verbraucherinformationen Deutschland vom 24.7.2017 [Deutsch]	ja, siehe Anmerkung	nein
		Cisco WebEx über Telekom	https://konferenzen.telekom.de/produkte-und-preise/telefon-und-web/cisco-webexr/	Auftragsverarbeitungsvertrag zum Vertrag über Cisco Webex (Webex Standard) Version 1.0 vom 15.01.2020 [Deutsch], Anhang AVV zum Vertrag über Telekommunikationsleistungen Version 2.2 vom 16.04.2020 [Deutsch]	ja, siehe Anmerkung Anbieter hat Änderungen angekündigt	nein, siehe Anmerkung
		frei verfügbare Jitsi-Angebote			in der Regel ja, da kein Auftragsverarbeitungsvertrag	

* Ergebnis der rechtlichen Bewertung der Auftragsverarbeitungsverträge. Einzelheiten der Bewertung in den Erläuterungen zu dem jeweiligen Dienst.

† Ergebnis der technischen Untersuchung der Dienste. Hinweise für Verantwortliche in den Erläuterungen zu dem jeweiligen Dienst.

		Google Meet (als Teil der G Suite unter Geltung des G Suite (Online) Agreement und des Data Processing Amendment to G Suite and/or Complimentary Product Agreement)	https://apps.google.com/meet/	G Suite (Online) Agreement Version 8 April 2020; Data Processing Amendment to G Suite and/or Complimentary Product Agreement, Version 2.2 [Englisch]	ja, siehe Anmerkung	nein
		Google Meet (kostenlos)	https://apps.google.com/meet/	Google-Nutzungsbedingungen, wirksam ab dem 31. März 2020, Google-Datenschutzerklärung, wirksam ab dem 31. März 2020 [Deutsch]	ja, kein Auftragsverarbeitungsvertrag	nein
		GoToMeeting	https://www.gotomeeting.com/de-de	Datenverarbeitungsnachtrag vom 26. Dezember 2019 [Deutsch]	ja, siehe Anmerkung	nein
		Microsoft Teams (als Teil von Microsoft 365 unter Gültigkeit der Online Service Terms)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste Januar 2020 [Deutsch] – Dateiversionen (laut Metadaten) vom 3.1.2020 und 9.6.2020 (Version ist im Dokument selbst nicht ersichtlich)	ja, siehe Anmerkung	nein
		Microsoft Teams (kostenlose Version)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Microsoft-Servicevertrag gültig ab 30. August 2019, Datenschutzerklärung von Microsoft April 2020 [Deutsch]	ja, kein Auftragsverarbeitungsvertrag	nein
		NETWAYS Web Services Jitsi	https://nws.netways.de/de/apps/jitsi/	AVV v1.7 [Deutsch]	keine gefunden	ja

		sichere-videokonferenz.de	https://sichere-videokonferenz.de/	Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung Stand 06/2020 [Deutsch]	keine gefunden	ja
		Skype	https://www.skype.com/de/	Microsoft-Servicevertrag gültig ab 30. August 2019, Datenschutzerklärung von Microsoft April 2020 [Deutsch]	ja, kein Auftragsverarbeitungsvertrag	nein
		Skype for Business Online (auslaufend, unter Gültigkeit der Online Service Terms)		Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste Januar 2020 [Deutsch] – Dateiversionen (laut Metadaten) vom 3.1.2020 und 9.6.2020 (Version ist im Dokument selbst nicht ersichtlich)	ja, siehe Anmerkung zu Microsoft Teams (als Teil von Microsoft 365 unter Gültigkeit der Online Service Terms)	nein
		TixeoCloud	https://www.tixeo.com	Vertrag zur Auftragsverarbeitung Version 20200608 [Deutsch]	keine gefunden	ja
		Werk21 BigBlueButton	https://www.werk21.de/produkte/co_working/bigbluebutton/index.html	Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO, Version 1.2.1., 06/2020 [Deutsch]	keine gefunden	ja
		Wire	https://wire.com/de/	Datenverarbeitungszusatz Juni 2020 [Deutsch]	keine gefunden	nein, auch Schweiz
		Zoom	https://zoom.us	Global Data Processing Addendum December 2019 [Englisch]	ja, siehe Anmerkung	nein

Anmerkungen zu den einzelnen Anbietern

Bitte beachten Sie, dass es über die hier angesprochenen Probleme hinaus weitere geben kann und die Nutzung der Dienste trotz Behebung der hier genannten Probleme unzulässig sein kann. Insbesondere sind bei manchen Anbietern einzelne Klauseln unklar oder widersprüchlich oder gar die Verträge insgesamt so schwer verständlich gestaltet, dass es zu Unklarheiten kommt, was genau vereinbart ist. In diesen Fällen können Verantwortliche ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO nicht nachkommen.

In *kursiv* haben wir den Anmerkungen zu allen Anbietern eine knappe Zusammenfassung der gefundenen rechtlichen Mängel vorangestellt.

Blizz

Anbieter behält sich die Verarbeitung von Auftragsdaten zu eigenen Zwecken vor. Mängel im Auftragsverarbeitungsvertrag. Unklare Regelungen zu möglichen Datenexporten.

Der „Blizz Auftragsverarbeitungsvertrag“ (folgend: „AVV“) sieht in Ziff. 2.9 Satz 1 zwar eine Verpflichtung zum Nachweis der Einhaltung datenschutzrechtlicher Verpflichtungen vor, doch Ziff. 2.9 Satz 2 AVV schränkt diese nach Art. 28 Abs. 3 lit. h DS-GVO zwingende Verpflichtung ein, indem dort eine Regelung enthalten ist, was TeamViewer bereitzustellen hat, wenn die Verpflichtung nach Ziff. 2.9 Satz 1 nicht erfüllt wird. Die Verpflichtung nach Ziff. 2.9 Satz 2 bleibt hinter den gesetzlichen Mindestanforderungen zurück. In jedem Fall können Verantwortliche so nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 2.9 Satz 4 AVV sieht eine Vergütungspflicht für jede Art von zusätzlichen Überprüfungen vor, es sei denn, das von TeamViewer (Anbieter von Blizz) bereitgestellte Zertifikat gibt begründeten Anlass zu Zweifeln an einer Einhaltung des Rechts. Jedenfalls dadurch, dass keine Ausnahmen für durch Vertragsverstöße erforderlich gewordene Überprüfungen gemacht werden, wird durch diese zunächst zivilrechtliche Regelung das Überprüfungsrecht weitgehend entwertet, sodass Art. 28 Abs. 3 lit. h DS-GVO verletzt ist.

Ziff. 2.13 AVV weckt Zweifel, ob Ziff. 2.2 AVV eingeschränkt werden soll, was das nach Art. 28 Abs. 3 lit. a DS-GVO zwingende Weisungsrecht hinsichtlich Datenexporten in Drittstaaten angeht.

Ziff. 3.1 AVV verweist für den Einsatz von weiteren Auftragsverarbeitern auf einen URL, der eine Liste aktuell eingesetzter Unterauftragsverarbeiter enthält, ohne aber auch eine Genehmigung dieser Unterauftragsverarbeiter zu enthalten. Darüber hinaus muss die Liste der Subunternehmer zum Zeitpunkt des Vertragsschlusses nicht mit einer eventuell durch den Auftraggeber gesichteten und/oder gesicherten Fassung übereinstimmen. Damit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) nachkommen.

TeamViewer (Anbieter von Blizz) behält sich unter Teil A Ziff. 3.9 der „Endnutzer-Lizenzvereinbarung – Blizz“ (folgend: „EULA“) die Verarbeitung eigentlich im Auftrag verarbeiteter personenbezogener Daten zu eigenen Zwecken vor. Teil A Ziff. 2.6 EULA sieht darüber hinaus eine Analyse (Tracking) des „Verhalten[s] des Kunden beim Verwenden des Produkts als auch [des] Online-Nutzungsverhalten[s]“ vor. Eine Rechtsgrundlage für die damit verbundene Offenlegung personenbezogener Daten durch Verantwortliche ist nicht ersichtlich. Aus der Verarbeitung der Auftragsdaten auch zu eigenen Zwecken von TeamViever folgt die Problematik einer gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO. Eine solche liegt

nach der Rechtsprechung des EuGH nahe, ist jedenfalls anhand der nur rudimentären Angaben im EULA nicht auszuschließen. Dies ist mindestens im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) ein Problem. Im Fall des tatsächlichen Vorliegens kommt hinzu, dass keine Vereinbarung nach Art. 26 DS-GVO besteht.

Cisco WebEx

Standardmäßig kein Auftragsverarbeitungsvertrag bei Online-Bestellung. Anbieter behält sich die Verarbeitung von Auftragsdaten zu eigenen Zwecken vor. Mängel im Auftragsverarbeitungsvertrag. Unzulässige Einschränkungen des Weisungsrechts. Unzulässige Datenexporte.

Standardmäßig wird jedenfalls bei Online-Buchung kein Auftragsverarbeitungsvertrag geschlossen, sondern nur die „Universelle Cloud-Vereinbarung“ und ggf. Reseller-AGB der Digital River Ireland Ltd. werden einbezogen.

Cisco behält sich unter Abschnitt 4.b und c der „Universellen Cloud-Vereinbarung“ Version 9.3 vom 15. April 2020 sowie unter Ziff. 8 des „Data Protection Exhibit, Attachment B“ zum „Master Data Protection Agreement“, Dezember 2019, die Verarbeitung eigentlich im Auftrag verarbeiteter personenbezogener Daten zu eigenen Zwecken vor.

Ziff. 4.c.ii des „Data Protection Exhibit, Attachment B“ zum „Master Data Protection Agreement“ sieht keine ausreichende Vertraulichkeitspflicht der zur Datenverarbeitung eingesetzten Personen vor. Durch Ziff. 4.c.ii und Ziff. 4.d.ii sollen offenbar Art. 48 DS-GVO und Art. 28 Abs. 3 lit. a DS-GVO unzulässig eingeschränkt werden, indem auch nach europäischem Recht unzulässige Offenlegungen an ausländische Behörden erlaubt werden. Ziff. 4.c.v gibt dem Verantwortlichen nur eine Möglichkeit zum Widerspruch gegen Datenexporte, die dann automatisch zum Entfallen der betroffene Leistungspflicht von Cisco führt, aber kein echtes Weisungsrecht nach Art. 28 Abs. 3 lit. a; Entsprechendes gilt für den Einsatz von weiteren Auftragsverarbeitern in Ziff. 6.b. Beide sehen nur ein automatisches Entfallen der Leistungspflicht von Cisco vor; unklar bleibt, ob die Vergütungspflicht des Auftraggebers bestehenbleibt, was das Widerspruchsrecht völlig entwerten würde. Ziff. 4.d.xii schränkt die Löschpflicht nach Abschluss der Erbringung der Verarbeitungsleistung stärker ein als nach Art. 28 Abs. 3 lit. g DS-GVO zulässig. Das Verhältnis von Ziff. 6.e zu Ziff. 6.b ist unklar, Cisco scheint sich hier im Verstoß gegen Art. 28 Abs. 2 DS-GVO die Einbeziehung von weiteren Auftragsverarbeitern ohne proaktive Information des Verantwortlichen und ohne Einspruchsrecht vorzubehalten.

Ziff. 4.c.v des „Data Protection Exhibit, Attachment B“ zum „Master Data Protection Agreement“ erlaubt Cisco Datenexporte in unsichere Drittstaaten und erklärt hierfür nur das Privacy Shield für (begrenzt) anwendbar, das allerdings nur für die USA gilt. Eine andere Rechtfertigung der Datenexporte wie Standardvertragsklauseln ist nicht vorgesehen.

Es besteht zwar eine Unklarheiten- und Vorrangregelung in Ziff. 2.d des „Data Protection Exhibit, Attachment B“ zum „Master Data Protection Agreement“, doch bezieht sich diese nur auf Unklarheiten und bereits aus dem Gesetz bestehende vorrangige gesetzliche Verpflichtungen von Cisco, während Art. 28 DS-GVO davon ausgeht, dass die dort genannten Verpflichtungen vertraglich begründet werden. Zudem ist das Ergebnis der Auslegung nicht sicher vorhersehbar, sodass Verantwortliche wegen der Unklarheiten im Vertrag nicht ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO nachkommen können.

Cisco WebEx Meetings über Telekom

Mängel im Auftragsverarbeitungsvertrag. Unzulässige Einschränkungen des Weisungsrechts. Unklare Regelungen zu Datenexporten.

§ 3 Abs. 3, 4 des „Auftragsverarbeitungsvertrags (AVV) zum Vertrag über Cisco Webex (Webex Standard)“, Version 1.0 vom 15.01.2020 (folgend: „AVV“) – im Wesentlichen wortgleich § 3 Abs. 4, 5 des „Anhangs AVV zum Vertrag über Telekommunikationsleistungen Version 2.2 vom 16.04.2020 [Deutsch]“ (folgend: „AVV2“) enthält entgegen Art. 28 Abs. 3 lit. h DS-

GVO keine ausreichend klare Verpflichtung, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung zu stellen. Zudem ist die offensichtlich fehlerhafte Kostenklausel in § 3 Abs. 2 UAbs. 2 AVV wohl so gemeint, dass sowohl die Einholung der Nachweise als auch jegliche Kontrollen kostenpflichtig sind, was durch die berichtigte Fassung in § 3 Abs. 3 UAbs. 3 AVV2 bestätigt wird. Jedenfalls eine Kostenpflichtigkeit der Erbringung der in Art. 28 Abs. 3 lit. h DS-GVO vorgesehenen Nachweise durch den Auftragsverarbeiter und von Kontrollen, die durch Verstöße des Auftragnehmers veranlasst sind, entwertet diese Pflichten und Rechte umfassend und verstößt daher gegen Art. 28 Abs. 3 lit. h DS-GVO. Es sollte – auch im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) – klargestellt werden, dass es im besonderen Einzelfall auch Kontrollen geben kann, bei denen die angemessene Ankündigungsfrist Null ist, d. h. ausnahmsweise keine vorherige Ankündigung erforderlich ist.

§ 4 Abs. 3 AVV (ebenso AVV2) sieht vor, dass der Ort der Datenverarbeitung in Annex 2 AVV (AVV2) geregelt wird. Dort fehlen jegliche Angaben zum Ort der Verarbeitung. Annex 4 AVV (AVV2) regelt – offenbar beschränkt auf Unterauftragsverarbeiter – die vereinbarten Leistungsländer. Die Angaben in Annex 4 AVV sind allerdings widersprüchlich, weil als „Ort der Leistung [Land]“ „United Kingdom, Feltham“ angegeben ist, allerdings als „Standorte der Cisco WebEx Meetings Rechenzentren“ „Amsterdam, Netherlands“ und „London, UK“ angegeben sind und als „Standorte der Cisco WebEx Service Rechenzentren (Webex Teams)“ diverse weitere Standorte auch in Drittstaaten ohne angemessenes Datenschutzniveau. Annex 4 AVV2 ist gegenüber Annex 4 AVV geändert und führt Unterauftragsverarbeiter auf, die ihre Leistungen in UK, USA und Singapur erbringen. Für Angaben zu den Standorten wird auf eine Website von Cisco verwiesen. Eine Differenzierung nach den verschiedenen Produkten erfolgt nur noch hinsichtlich weiterer Informationen. Annex 5 AVV nennt zudem diverse „Genehmigte Sub-Unterauftragsverarbeiter“ insbesondere in den USA. Annex 4 Ziff. (3) AVV verweist auf auch im Namen des Verantwortlichen abgeschlossene Standardvertragsklauseln und ein „Supplementary Agreement to the EU Standard Contractual Clauses“. Dieses lag uns nicht vor. Es ist durch die Verantwortlichen kritisch zu prüfen, ob diese Zusatzvereinbarung auch nur geringste Einschränkungen der Standardvertragsklauseln enthält, was dazu führen würde, dass der Datenexport nicht mehr durch die Standardvertragsklauseln gerechtfertigt werden können. Im Rahmen der Beratung von Verantwortlichen wurde uns von diesen mitgeteilt, dass angeblich für WebEx Meetings die Datenverarbeitung auf EU und Großbritannien beschränkt sei. Es gibt Hinweise im AVV, dass dies tatsächlich gewollt sein könnte; der AVV bildet dies aber nicht korrekt ab. Aus dem AVV2 ergeben sich derartige Hinweise nicht mehr. Annex 5 AVV2 verweist für genehmigte Sub-Unterauftragsverarbeiter auf Dokumente von Cisco. Die Liste der Sub-Unterauftragsverarbeiter zum Zeitpunkt des Vertragsschlusses muss nicht mit einer eventuell durch den Auftraggeber gesichteten und/oder gesicherten Fassung übereinstimmen. Damit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) nachkommen. Zudem ist unklar, ob bei Änderungen der Sub-Unterauftragsverarbeiter eine proaktive Vorab-Information der Verantwortlichen erfolgt, wie von Art. 28 Abs. 2 Satz 2 DS-GVO zwingend verlangt.

§ 4 Abs. 12 AVV (ebenso AVV2) schränkt die Löschpflicht nach Auftragserledigung entgegen Art. 28 Abs. 3 lit. g DS-GVO ein, indem die Löschpflicht unzulässig auch aufgrund von Nicht-EU-/Nicht-mitgliedstaatlichem Recht ausgeschlossen wird, das Wahlrecht des Verantwortlichen fehlt und es besteht ein im Einzelnen zu prüfender Vorbehalt. Das Verhältnis zu § 4 Abs. 13 AVV/AVV2 ist unklar, und auch dort bestehen vergleichbare Probleme.

§ 5 Abs. 1 (ebenso AVV2) AVV genügt nicht den Anforderungen des Art. 28 Abs. 3 lit. c DS-GVO, weil die Telekom nicht zur Einhaltung der nach Art. 32 DS-GVO erforderlichen technisch-organisatorischen Maßnahmen verpflichtet ist.

Die Regelung der Information über neue Unterauftragsverarbeiter in § 7 Abs. 4 AVV (ebenso AVV2) stellt nicht sicher, dass die Information proaktiv erfolgt, was nach Art. 28 Abs. 2 Satz 2 DS-GVO erforderlich wäre. Damit können Verantwortliche zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen. Ebenfalls ist

der Maßstab für Einsprüche gegen den Einsatz von Unterauftragsverarbeitern zu streng und entwertet das Einspruchsrecht aus Art. 28 Abs. 2 Satz 2 DS-GVO.

Annex 2 AVV (ebenso AVV2) enthält nicht alle Datentypen und Betroffenen, deren Daten im Auftrag verarbeitet werden; enthalten sind dafür Angaben, die sich wohl nicht auf die Auftragsverarbeitung beziehen dürften, sondern auf die Verarbeitung durch den Auftragnehmer in eigener Verantwortlichkeit.

Der AVV – weniger der AVV2 – enthält insgesamt eine Reihe kleinerer Fehler und Unklarheiten, die vor dem Hintergrund der Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) vor einer Nutzung beseitigt werden müssten.

Google Meet (als Teil der G Suite unter Geltung des G Suite (Online) Agreement und des Data Processing Amendment to G Suite and/or Complimentary Product Agreement)

Mängel im Auftragsverarbeitungsvertrag. Unzulässige Einschränkungen des Weisungsrechts. Unzulässige Datenexporte.

Ziff. 6.1 des „Data Processing Amendment to G Suite and/or Complimentary Product Agreement, Version 2.2“ (folgend: „DPA“) schränkt das Weisungsrecht hinsichtlich der Datenlöschung und die Benachrichtigungspflicht entgegen Art. 28 Abs. 3 lit. a DS-GVO ein, indem Google sich eine Löschfrist von 180 Tagen einräumt und zudem die Löschpflicht unzulässig auch aufgrund von mitgliedstaatlichem Recht ausschließt, dem Google nicht unterliegt. Die Löschpflicht nach Auftragserledigung nach Art. 28 Abs. 3 lit. g DS-GVO wird durch Ziff. 6.2 DPA unzulässig eingeschränkt, indem Google sich auch insoweit eine Löschfrist von 180 Tagen einräumt.

Das DPA enthält entgegen Art. 28 Abs. 3 lit. h DS-GVO keine umfassende Verpflichtung für Google, den Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung zu stellen. Ziff. 7.5.1, 7.5.3.a und 7.5.3.b DPA sehen nur ein beschränktes Einsichtsrecht in bestimmte durch Google beauftragte Reports vor.

Ziff. 7.5.3.c DPA sieht eine Vergütungspflicht für jede Art von Überprüfungen durch Verantwortliche vor. Jedenfalls dadurch, dass keine Ausnahmen für durch Vertragsverstöße erforderlich gewordene Überprüfungen gemacht werden, wird durch diese zunächst zivilrechtliche Regelung das Überprüfungsrecht weitgehend entwertet, sodass Art. 28 Abs. 3 lit. h DS-GVO verletzt ist.

Ziff. 10.2.1.a DPA sieht den Abschluss von Standardvertragsklauseln für Datenexporte nur auf Verlangen des Kunden vor, wobei Ziff. 10.1 DPA eine Datenverarbeitung überall dort erlaubt, wo Google oder seine Unterauftragsverarbeiter Einrichtungen unterhalten.

Das Verfahren zur Information über gegenwärtige Unterauftragsverarbeiter in Ziff. 11.1 DPA stellt nicht sicher, dass Verantwortliche nachweisen (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) können, welche Unterauftragsverarbeiter mit Vertragsschluss genehmigt wurden. Googles „Affiliates“ sind pauschal als Unterauftragsverarbeiter erlaubt, wobei der Begriff dynamisch definiert ist. Durch gesellschaftsrechtliche Änderungen kann es damit zur Einbeziehung weiterer Unterauftragsverarbeiter kommen, ohne dass Verantwortliche hiergegen ein Widerspruchsrecht haben, wie nach Art. 28 Abs. 2 Satz 1 DS-GVO zwingend erforderlich.

Ziff. 11.3.a.ii DPA stellt nicht sicher, dass – wie von Art. 28 Abs. 4 Satz 1 DS-GVO verlangt – weiteren Auftragsverarbeitern dieselben Datenschutzpflichten auferlegt werden, die im DPA festgelegt sind, sondern beschränkt dies auf Verpflichtungen, die in Art. 28 Abs. 3 DS-GVO beschrieben sind.

Die Beschreibung der Information über neue Unterauftragsverarbeiter in Ziff. 11.4 DPA ist jedenfalls im Zusammenspiel mit Ziff. 11.2 DPA unklar, weil sie auch so ausgelegt werden kann, dass die Information nicht proaktiv erfolgt, sondern nur über eine Website, was nach Art. 28 Abs. 2 Satz 2 DS-GVO nicht genügt. Damit können Verantwortliche zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 13 DPA beschränkt die Verpflichtungen aus den Standardvertragsklauseln unzulässig, sodass diese nicht zur Rechtfertigung des Datenexports herangezogen werden können. Konkret beschränkt wird die Haftung aus Ziff. 6.2 der Standardvertragsklauseln, weil unter den Begriff der Affiliates in Ziff. 13.1 DPA auch eine natürliche Person fallen kann, die nicht selbst Vertragspartner oder Verantwortlicher ist. Zudem verweist Ziff. 13.2 ergänzend auf Ziff. 13 des „G Suite (Online) Agreement", das in Ziff. 13.1.a und b jegliche Haftung im Zusammenhang mit dem Nutzungsvertrag einschränkt, und zwar nicht beschränkt auf die Parteien. Die salvatorische Klausel in Ziff. 13.2 des „G Suite (Online) Agreement" umfasst – unabhängig von der Frage, ob salvatorische Klauseln für Haftungsausschlüsse überhaupt zulässig sind – nur solche Angelegenheiten, für die eine Haftungsbegrenzung bzw. ein Haftungsausschluss gesetzlich ausgeschlossen sind. Die Haftung nach Ziff. 6.2 der Standardvertragsklauseln stellt aber eine vertragliche Haftungsübernahme dar, die über die gesetzliche Haftung hinausgeht.

Hinweis (nicht notwendig Mangel): Es ist im Einzelfall zu prüfen, ob die in Ziff. 7.1.1 DPA abschließend definierten technisch-organisatorischen Maßnahmen den Anforderungen des Art. 32 DS-GVO genügen. Darüber hinaus enthält das DPA Klauseln, die noch einer genaueren Bewertung bedürfen.

GoToMeeting

Mängel im Auftragsverarbeitungsvertrag. Unzulässig beschränkter Anwendungsbereich. Unzulässige Datenexporte.

Ziff. 5.1 des „Datenverarbeitungsnachtrags" vom 26. Dezember 2019 sieht entgegen Art. 28 Abs. 4 Satz 1 DS-GVO Überprüfungen bei Unterauftragnehmern und vertragliche Vereinbarungen mit diesen nur dann vor, wenn es sich nicht um Konzernunternehmen von LogMeIn handelt. Zudem müssen entgegen Art. 28 Abs. 4 Satz 1 DS-GVO die vertraglichen Datenschutz-Verpflichtungen nur „im Wesentlichen" auch den Unterauftragnehmern auferlegt werden.

Das Verfahren zur Information über gegenwärtige Unterauftragsverarbeiter in Ziff. 5.2 des „Datenverarbeitungsnachtrags" stellt nicht sicher, dass Verantwortliche nachweisen (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) können, welche Unterauftragsverarbeiter mit Vertragsschluss genehmigt wurden. Das Verfahren zur Information über neue Unterauftragsverarbeiter in Ziff. 5.2 erfordert ein aktives Handeln der Verantwortlichen und genügt damit nicht Art. 28 Abs. 2 Satz 2 DS-GVO. Verantwortliche, die die Benachrichtigungen nicht selbst aktiv abonnieren, können zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 6.2 des „Datenverarbeitungsnachtrags" genügt nicht den Anforderungen des Art. 28 Abs. 3 lit. h DS-GVO an Nachweispflichten und Kontrollrechte.

Ziff. 10 des „Datenverarbeitungsnachtrags" beschränkt die Anwendbarkeit bestimmter, in diesem Abschnitt genannter, zwingend erforderlicher Regelungen auf einen Ausschnitt der Verarbeitungen personenbezogener Daten, die der DS-GVO unterliegen; Art. 3 DS-GVO ist viel weiter.

Ziff. 10.3 i. V. m. Anhang 1 des „Datenverarbeitungsnachtrags" sieht Einschränkungen der Standardvertragsklauseln vor, die zwar wegen einer Vorrangregelung für die Standardvertragsklauseln in Ziff. 12 zivilrechtlich nicht gelten dürften, aber dennoch zu einer unzulässigen Abwandlung führen, sodass diese den Datenexport nicht rechtfertigen können. Die Selbstzertifizierung nach dem Privacy Shield bezieht sich nicht auf HR-Daten.

Microsoft Teams (als Teil von Microsoft 365 unter Gültigkeit der Online Service Terms)

Anbieter behält sich die Verarbeitung von Auftragsdaten zu eigenen Zwecken vor. Mängel im Auftragsverarbeitungsvertrag. Viele Unklarheiten und Widersprüche im Auftragsverarbeitungsvertrag. Unzulässige Datenexporte. Anbieter hat veröffentlichten Auftragsverarbeitungsvertrag ohne Kennzeichnung umfangreich nachträglich geändert; Version (laut Metadaten) vom 3.1.2020 enthält unzulässige Einschränkungen des Weisungsrechts.

Wichtiger Hinweis: Microsoft hat den „Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste (Deutsch, Januar 2020)“ (folgend: „DPA“) ohne Kennzeichnung nachträglich umfangreich geändert. Es gibt ein Dokument, das ausweislich der Metainformationen am 3.1.2020 erstellt wurde und ein Dokument, das ausweislich der Metainformationen am 9.6.2020 erstellt wurde. Die Bezeichnung der Dokumente ist gleich, das von Microsoft im Internet veröffentlichte Dokument wurde stillschweigend ersetzt. In der Änderungshistorie („Verdeutlichungen und Zusammenfassung der Änderungen“) steht ausdrücklich „Keine“, obwohl große Teile des Vertrags geändert wurden. Die meisten dieser Änderungen sind rein sprachlicher Art. Insbesondere wurde in der Version vom 9.6.2020 die Anlage Standardvertragsklauseln, die ursprünglich sehr umfangreiche Abweichungen vom Wortlaut der genehmigten Standardvertragsklauseln enthielt, im Wesentlichen dem genehmigten Text angepasst. Allerdings gibt es auch relevante inhaltliche Änderungen. Die meisten Änderungen sind positiv zu bewerten. Dennoch bleibt eins der wichtigsten Grundprobleme des Vertrags, dass er an vielen Stellen unklar und widersprüchlich ist, bestehen.

Microsoft behält sich im DPA unter dem Punkt „Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse“ die Verarbeitung eigentlich im Auftrag verarbeiteter personenbezogener Daten zu eigenen Zwecken vor. Eine Rechtsgrundlage für die damit verbundene Offenlegung personenbezogener Daten durch den Verantwortlichen an Microsoft ist nicht ersichtlich. Aus der Verarbeitung der Auftragsdaten auch zu eigenen Zwecken von Microsoft folgt die Problematik einer gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO. Eine solche liegt nach der Rechtsprechung des EuGH nahe, ist jedenfalls anhand der nur rudimentären Angaben im DPA nicht auszuschließen. Dies ist mindestens im Hinblick auf die Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) ein Problem. Im Fall des tatsächlichen Vorliegens kommt hinzu, dass keine Vereinbarung nach Art. 26 DS-GVO besteht.

Das DPA enthält an vielen Stellen Regelungen, die den gesetzlichen Mindestanforderungen widersprechen. Es gibt allerdings im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO“ einen in seiner Bedeutung unklaren Verweis auf Anlage 3 zum DPA, die wiederum wesentliche Inhalte aus den Art. 28, 32 und 33 DS-GVO wiedergibt, aber ebenfalls im Unklaren lässt, ob diese Regeln nun für Microsoft verpflichtend dem eigentlichen – klar rechtswidrigen – Text des DPA vorgehen sollen oder nicht. Die Datei-Version vom 9.6.2020 verschlechtert diese Klausel sogar noch, indem sie nun von „[den] personenbezogenen Daten der DSGVO“ spricht. Ein derartig unklarer Auftragsverarbeitungsvertrag macht es den Verantwortlichen unmöglich, ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO nachzukommen.

Aber auch Anlage 3 zum DPA (in der Datei-Fassung vom 3.1.2020) übernimmt den relevanten Wortlaut des Art. 28 DS-GVO nicht vollständig. Jedenfalls Ziff. 2 lit. g der Anlage 3 (in der Datei-Fassung vom 3.1.2020) bleibt hinter den gesetzlichen Mindestanforderungen des Art. 28 Abs. 3 lit. g DS-GVO zurück, indem eine Löschung oder Rückgabe der Auftragsdaten nach Auftragsende nur auf Wunsch des Kunden vorgesehen ist und nicht in jedem Fall. Ziff. 2 lit. a der Anlage 3 (in der Datei-Fassung vom 3.1.2020) schränkt zudem das Weisungsrecht des Kunden unzulässig entgegen Art. 28 Abs. 3 lit. a DS-GVO ein, weil Ausnahmen nicht nur aufgrund des Unionsrechts oder des Rechts der Mitgliedstaaten, dem Microsoft unterliegt, vorgesehen ist. In der Datei-Fassung vom 9.6.2020 sind diese Mängel stillschweigend behoben worden, ebenso wie der Wortlaut der Anlage weiter an den Wortlaut des Gesetzes angenähert wurde. Allerdings wurde auch teilweise der Wortlaut des Gesetzes aus der Version vom 3.1.2020 in der Version vom 9.6.2020 durch eigene Begriffe ersetzt. Zudem wurde eine neue Abweichung von den Mindestanforderungen des Art. 28 Abs. 3 lit. a DS-GVO eingefügt, indem die Pflicht zur Benachrichtigung des Kunden, wenn Microsoft zur weisungswidrigen Datenverarbeitung verpflichtet ist, nicht nur aufgrund des für die Verarbeitungspflicht maßgeblichen Rechts, sondern aufgrund jeden Rechts (Wortlaut „die Gesetzgebung“) ausgeschlossen wird. Eine weitere Abweichung zu Lasten des Kunden in der Neufassung vom 9.6.2020 von Ziff. 7 der Anlage 3 ist, dass Microsoft die für die Meldung einer sog. Datenpanne erforderlichen Informationen nur noch dann dem Kunden zur Verfügung stellen

muss, sofern (statt soweit, also nunmehr nur noch dann, wenn die Bedingung für alle Informationen erfüllt ist und nicht mehr wie vorher teilweise, wenn die Bedingung für Teile der Informationen erfüllt ist) diese Informationen Microsoft nach billigem Ermessen zur Verfügung stehen (statt der objektiven Formulierung „in angemessener Weise“ also nunmehr auf eine nur beschränkt gerichtlich überprüfbare Billigkeitsentscheidung von Microsoft abstellend). Es ist zudem nicht ersichtlich und aufgrund der versteckten Änderung des Vertrags durch Microsoft nicht zu erwarten, dass diese neue Fassung des Vertrags auch mit Bestandskunden vereinbart worden ist.

Im DPA sind unter dem Punkt „Datensicherheit – Prüfung der Einhaltung“ Einschränkungen der Standardvertragsklauseln vorgesehen. Diese werden als „Zusatz zu Klausel 5, Absatz f und Klausel 12, Absatz 2 der Standardvertragsklauseln“ bezeichnet und es wird behauptet, die Standardvertragsklauseln würden hierdurch nicht abgeändert. Zwar besteht in der Einleitung des DPA eine allgemeine Aussage, dass die Standardvertragsklauseln dem DPA vorgehen, wie auch die Standardvertragsklauseln mit ihrem Abänderungsverbot selbst eine entsprechende Vorrangregelung enthalten. Fraglich – und im Hinblick auf Art. 5 Abs. 2 DS-GVO problematisch – ist bereits, ob die allgemeine Vorrangklausel in der Einleitung des DPA überhaupt anwendbar ist, wenn die in Rede stehende konkrete Einschränkung der Standardvertragsklauseln selbst von sich behauptet, keine Einschränkung darzustellen, sodass unter dieser Annahme die Vorrangklausel denklogisch nicht zur Anwendung kommen kann. Dies kann allerdings offenbleiben, weil jede Einschränkung der Rechte und Pflichten aus den Standardvertragsklauseln, unabhängig von ihrer Formulierung und auch wenn sie an anderer Stelle für nachrangig und damit nicht anwendbar erklärt wird, zu einer unzulässigen Abwandlung der Standardvertragsklauseln führt. Denn damit wird bezweckt und im Ergebnis regelmäßig auch erreicht, dass die Standardvertragsklauseln nicht vollständig angewendet werden können. Dementsprechend betont auch Erwägungsgrund 109 DS-GVO, dass sonstige Vertragsklauseln weder mittelbar noch unmittelbar im Widerspruch zu den Standard-Datenschutzklauseln stehen dürfen. Somit führt auch die vorliegende Einschränkungs-„Zusatz“-Klausel trotz ihrer mutmaßlichen zivilrechtlichen Unwirksamkeit zu einer unzulässigen Abwandlung der Standardvertragsklauseln, sodass diese den Datenexport nicht rechtfertigen können. Microsoft hat sich zwar zusätzlich einer Selbstzertifizierung nach dem Privacy Shield unterworfen, doch gilt dieses nur für die USA. Microsoft behält sich aber eine Verarbeitung der Auftragsdaten an jedem Ort vor, an dem Microsoft oder seine Unterauftragsverarbeiter tätig sind (DPA, Abschnitt „Datenschutzbestimmungen – Datenübermittlungen und Speicherstelle – Datenübermittlungen“).

Wir weisen darauf hin, dass wir angesichts der nachträglichen nicht dokumentierten Änderung des veröffentlichten Auftragsverarbeitungsvertrags durch Microsoft bei Prüfungen beabsichtigen, auch die Einhaltung der Form des Auftragsverarbeitungsvertrags gemäß Art. 28 Abs. 9 DS-GVO und die entsprechende Nachweisbarkeit (Art. 5 Abs. 2 DS-GVO) zu prüfen.

NETWAYS Web Services Jitsi[3]

Bei dem Angebot von Netways erhält man Moderator-Zugriff auf eine vorkonfigurierte Instanz von Jitsi Meet. Das vorkonfigurierte Passwort ist lang, kann aber nicht selbst verändert werden. Bevor die Konferenz durch die/den Moderator/-in eröffnet wurde, ist es nicht möglich, ihr beizutreten. In der Standardkonfiguration sind die Konferenzen nicht durch Passwort geschützt und die Teilnehmenden betreten die Konferenz mit aktiver Kamera und aktivem Mikrofon.

[3] Bei Jitsi Meet handelt es sich um freie und quelloffene Software. Wir haben beispielhaft die Angebote zweier Dienstleister betrachtet, die den Betrieb der Software zum Inhalt haben und uns im Zuge unserer Beratungstätigkeit bekannt wurden. Am Markt sind eine Reihe weiterer Betreiber dieser Software tätig. Mit der Nennung der Anbieter ist keine Aussage dahingehend verbunden, dass ihre Dienstleistung der anderer im Wettbewerb stehender Unternehmen vorzuziehen ist.

Verantwortliche sollten daher vor dem Starttermin und bevor andere Teilnehmende die Konferenz betreten die Konferenz eröffnen und ein Passwort setzen. Zudem sollten Verantwortliche in den Einstellungen unter dem Reiter „Mehr“ aktivieren, dass bei neu hinzukommenden Teilnehmenden Mikrofon und Kamera deaktiviert sind.

Ein besonderes Augenmerk sollte auf die Authentifizierung der Teilnehmenden gelegt werden, da zum Betreten einer Konferenz die Adresse, unter der diese betrieben wird, und – falls gesetzt – ein Passwort genügen. Ein Sicherheitsgewinn kann somit erzielt werden, wenn das Passwort auf einem anderen Kanal als der Einladungslink kommuniziert wird.

Bei der Verwendung der Jitsi-App empfiehlt sich, zumindest auf Android-Geräten die Variante aus dem F-Droid-Store zu nutzen, da diese im Gegensatz zu der Variante aus dem Google-Play-Store frei von Software von Tracking-Anbietern wie Crashlytics und Firebase ist.

sichere-videokonferenz.de

Das Angebot von „Sichere Videokonferenz“ verfügt über keine Nutzendenverwaltung. Moderator/-in einer Konferenz wird automatisch die erste Person, die den Konferenzraum betritt. Daher müssen Verantwortliche besondere Sorge dafür tragen, dass sie die Konferenz eröffnen. Möglich wäre dies beispielsweise, indem der Link zu der Videokonferenz erst direkt zu Konferenzbeginn und nach Eröffnung der Konferenz versandt wird. Abgesehen davon gelten dieselben Empfehlungen wie für das Angebot von NETWAYS, da ebenfalls Jitsi Meet genutzt wird.

Tixeo Cloud

Für die Nutzung des Angebots von Tixeo ist zwingend eine Registrierung erforderlich. Da für die Registrierung die Nutzung einer E-Mail-Adresse erforderlich ist, bietet Tixeo gegenüber z. B. Jitsi eine etwas höhere Sicherheit hinsichtlich der Identität der Teilnehmenden. Hinzu kommt, dass einem geplanten Meeting nur eingeladene Teilnehmende beitreten können, was den Verantwortlichen eine gewisse Kontrolle über den Kreis der Teilnehmenden ermöglicht.

Tixeo Cloud erfordert die Installation eines Clients auf dem Gerät, auf dem es verwendet werden soll. Eine Nutzung über eine Webseite ist bei diesem Angebot nicht vorgesehen. Es muss also berücksichtigt werden, ob eine Installation von Software in der intendierten Umgebung möglich ist.

Der Veranstalter eines Meetings hat die Möglichkeit, den Teilnehmenden die Rechte für die Nutzung von Kamera und Mikrofon zu gewähren und zu entziehen. Die Funktion entspricht dabei der Kamera- und Mute-Funktion der jeweiligen Teilnehmenden. Werden die Rechte einer teilnehmenden Person wieder erteilt, wird sie in den Zustand versetzt, den sie vor dem Entzug der Rechte hatte. Dies sollte den Teilnehmenden mitgeteilt werden, da, sobald die Rechte entzogen sind, die jeweiligen Buttons verschwinden und somit die/der Moderator/-in die Eingabegeräte einschalten kann, wenn sie vor dem Rechteentzug eingeschaltet waren. Soll diese Funktion genutzt werden, sollten die Teilnehmenden vor Entzug der Rechte darauf hingewiesen werden, dass sie selbst ihre Kamera bzw. ihr Mikrofon deaktivieren sollten, sodass sie selbst auch nach Erteilung der Rechte selbst bestimmen können, wann die Eingabegeräte wieder aktiviert werden.

Werk21 – BigBlueButton[4]

Bei dem von Werk21 bereitgestellten Angebot erhalten Verantwortliche einen Zugang mit Moderator-Rechten auf einer BigBlueButton-Instanz. Für BigBlueButton ist derzeit nur der Zugriff über einen Internetbrowser möglich.

[4] Für BigBlueButton gilt das oben zu Jitsi Meet Gesagte entsprechend.

Teilnehmende benötigen zum Betreten der Videokonferenz in den Voreinstellungen nur die Adresse (URL) der Konferenz und betreten diese mit aktiviertem Mikrofon und deaktivierter Kamera. Verantwortliche sollten daher für die verwendeten Konferenzräume konfigurieren, dass ein zusätzlicher Zugangscode erforderlich ist und dass Teilnehmende mit deaktiviertem Mikrofon die Konferenz betreten. Zusätzlich ist es möglich, dass eine Freigabe durch die/den Moderator/-in erfolgen muss.

In den Voreinstellungen wird die Videokonferenz erst gestartet, nachdem die/der Moderator/-in sie eröffnet hat. Es ist aber möglich, auch anderen Teilnehmenden die Eröffnung zu erlauben oder alle Teilnehmenden zu Moderator/-innen zu machen. Besonders Letzteres sollte allerdings vermieden werden.

Soll die Funktion für das Erstellen von Aufnahmen genutzt werden, muss dies vorher mit den Teilnehmenden der Videokonferenz abgestimmt und müssen ggf. Einwilligungen eingeholt werden.

Wire

Im Angebot von Wire gibt es keine Möglichkeiten zur Moderation der eigentlichen Videokonferenzen. Gruppenmoderator/-innen haben lediglich die Möglichkeit, andere Personen aus der Gruppe zu entfernen. Der Ausschluss einer Person aus einer Gruppe entfernt diese aber nicht aus bereits laufenden Videoanrufen. Kontrolle über die Aktivierung/Deaktivierung der Kamera oder des Mikrofons haben die Teilnehmenden selbst. Auch bei Wire starten die Teilnehmenden einer Videokonferenz mit aktivierten Eingabegeräten.

Da die Nutzung von Wire zur Kommunikation die Mitgliedschaft in einem Team voraussetzt, haben Verantwortliche allerdings direkte Kontrolle darüber, welche Personen im Kontext der Anwendung miteinander kommunizieren können.

Verantwortliche müssen sicherstellen, dass durch Wire Metadaten über die Konferenzteilnahme nicht länger aufbewahrt werden, als es für die Zwecke der Verantwortlichen erforderlich ist.

Zoom

Mängel im Auftragsverarbeitungsvertrag. Unzulässige Einschränkungen der Löschpflicht. Unzulässige Datenexporte. Zweifel an der Zuverlässigkeit des Anbieters.

Ziff. 3.4 Satz 1 des „Zoom Global Data Processing Addendum“, December 2019 (folgend: „DPA“) schließt die Löschung der verarbeiteten personenbezogenen Daten nach Vertragsende in größerem Umfang aus als nach Art. 28 Abs. 3 lit. g DS-GVO zulässig, indem jedes beliebige auf Zoom bzw. Unterauftragsverarbeiter anwendbare Recht eine Nichtlöschung rechtfertigt.

Ziff. 3.4 Satz 2 und Ziff. 4.3 DPA könnten als Spezialregelungen Ziff. 6 DPA vorgehen, widersprechen jedenfalls Ziff. 6 DPA. Ziff. 6 DPA darf allerdings nicht eingeschränkt werden, da sonst ein Verstoß gegen Art. 32 DS-GVO vorliegen würde. Damit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 5.1 Satz 1 DPA verweist für den Einsatz von weiteren Auftragsverarbeitern auf einen URL, der eine Liste genehmigter Unterauftragsverarbeiter enthält, und sieht insoweit einen Aktualisierungsvorbehalt vor, wobei nicht eindeutig ist, ob sich der Aktualisierungsvorbehalt auf URL oder Inhalt beziehen soll. Durch diese Unklarheit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen. Darüber hinaus muss die Liste der Subunternehmer zum Zeitpunkt des Vertragsschlusses nicht mit einer eventuell durch den Auftraggeber gesichteten und/oder gesicherten Fassung übereinstimmen, und es nicht einmal geregelt, ob relevanter Zeitpunkt derjenige der Unterzeichnung durch den Verantwortlichen ist oder derjenige der Unterzeichnung durch Zoom. Damit können Verantwortliche zumindest nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a) nachkommen.

Das Verfahren zur Information über neue Unterauftragsverarbeiter in Ziff. 5.1 Satz 2 und 3 DPA erfordert ein aktives Handeln der Verantwortlichen und genügt damit nicht Art. 28 Abs. 2 Satz 2 DS-GVO. Verantwortliche, die die Benachrichtigungen nicht selbst aktiv abonnieren, können zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO) nachkommen.

Ziff. 5.2.1 DPA macht es Verantwortlichen faktisch unmöglich, gegen neue Unterauftragsverarbeiter Einspruch einzulegen, weil sie nur ein Kündigungsrecht für das DPA haben, aber ihre Zahlungsverpflichtungen nach dem Hauptvertrag fortbestehen. Dies entwertet das Einspruchsrecht vollständig, sodass ein Verstoß gegen Art. 28 Abs. 2 Satz 2 DS-GVO vorliegt.

Ziff. 9.3 und 9.4 DPA verstoßen gegen Art. 28 Abs. 3 lit. h DS-GVO. Es besteht keine umfassende Verpflichtung für Zoom, Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung zu stellen. Das einzige Recht, das es (unzulässig eingeschränkt, weil stets eine Vorankündigung verlangt wird, auch im Eilfall, und nur einmal jährlich, auch wenn zwischenzeitlich die Verarbeitung geändert wurde) gibt, ist das, sich Unterlagen im Büro von Zoom anzuschauen; außerdem maximal einmal jährlich eine Kopie nicht näher bezeichneter Zertifikate/Reports. Jegliches Recht zu eigenen Überprüfungen, die über die Einsicht in Unterlagen hinausgehen, insbesondere zur Vor-Ort-Kontrolle, ist ausgeschlossen.

In Ziff. 3.4 letzter Satz, 5.6 am Ende und 9.4 DPA werden die Standardvertragsklauseln unzulässig abgewandelt, sodass diese den Datenexport nicht rechtfertigen können (unabhängig von der Frage, ob diese Abwandlung zivilrechtlich wirksam ist oder nicht). Die Selbstzertifizierung nach dem Privacy Shield bezieht sich nicht auf HR-Daten.

Wir weisen darauf hin, dass Art. 28 Abs. 1 DS-GVO vorschreibt, dass nur Auftragsverarbeiter eingeschaltet werden dürfen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Bei der Prüfung von Verantwortlichen, die Zoom einsetzen, beabsichtigen wir, auf diesen Aspekt besonderes Augenmerk zu legen. Verantwortliche müssen vor einem Einsatz nachweisen können (Art. 5 Abs. 2 DS-GVO), dass Zoom diese Anforderungen mittlerweile erfüllt.

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

3. April 2020

Hinweise zum datenschutzkonformen Einsatz von digitalen Lernplattformen durch Schulen

Die Vorsorgemaßnahmen zur Eindämmung der Corona-Pandemie führen in nahezu allen Lebensbereichen zu Einschränkungen. Wegen der aktuellen Schulschließungen stehen die Berliner Schulen und deren Lehrpersonal vor der Herausforderung, den Schülerinnen und Schülern auch in dieser Zeit, in der ein regulärer Unterricht nicht möglich ist, Lern- und Unterrichtsmaterialien zur Verfügung zu stellen und Wege zu finden, um mit diesen in Austausch treten zu können. Dass die Berliner Schulen neue digitale Wege gehen und hierbei auch den Einsatz von Online-Lernplattformen zur Bereitstellung von Lerninhalten in den Blick nehmen, begrüßen wir grundsätzlich. Wichtig ist jedoch, dass hierbei die Persönlichkeitsrechte der Berliner Schülerinnen und Schüler gewahrt bleiben. Dies gilt insbesondere vor dem Hintergrund, dass Kinder und Jugendliche in besonderem Maße von der Datenschutz-Grundverordnung geschützt werden.

Man muss sich klarmachen, dass der Einsatz von digitalen Lernplattformen nicht zu unterschätzende Gefahren für die Persönlichkeitsrechte sowohl von Schülerinnen und Schülern als auch von Lehrkräften mit sich bringen kann. So setzt die Nutzung entsprechender Plattformen in der Regel eine personalisierte Anmeldung voraus. Teilweise werden Daten erhoben, die für die Nutzung der Plattform gar nicht benötigt werden. Anbieter der Plattformen können häufig das Nutzungsverhalten der angemeldeten Schülerinnen und Schüler sehr genau auswerten. Als Folge können Persönlichkeitsprofile über die Schülerinnen und Schüler, aber unter Umständen auch der Lehrkräfte, entstehen, die von den Anbietern für wirtschaftliche Zwecke, wie zum Beispiel Werbung, genutzt werden können. Fehlende Löschfunktionen bergen die Gefahr, dass Daten, die längst nicht mehr für pädagogische Aufgaben erforderlich sind, dauerhaft gespeichert bleiben und zu einem späteren Zeitpunkt zum Nachteil der Schülerinnen und Schüler genutzt werden können. Gerade bei privaten Anbietern, die ihren Sitz außerhalb der Europäischen Union haben, beispielsweise US-Anbieter, besteht zudem die Gefahr, dass Zugriffe von Behörden auf die Daten erfolgen können, die nach Europäischem Datenschutzrecht nicht zulässig wären. Es ist daher notwendig, bei der Auswahl digitaler Lernplattformen sehr genau darauf zu achten, wie die datenschutzrechtlichen Anforderungen umgesetzt werden.

Derzeit gibt es in Berlin verschiedene Angebote, die durchgängig nicht auf datenschutzgerechte Ausgestaltung überprüft sind. Dies gilt auch für den „Lernraum Berlin“ der Senatsverwaltung für Bildung, Jugend und Familie, der den Berliner Schulen bereits als Online-Plattform zur Verfügung steht. Hinsichtlich der Umsetzung der für diese Plattform geltenden datenschutzrechtlichen Vorgaben stehen wir jedoch bereits im Kontakt mit der verantwortlichen Senatsverwaltung. Daneben wird von privaten Anbietern, wie beispielsweise Schulbuchverlagen, eine Vielzahl verschiedener Online-Lernplattformen angeboten.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit möchte daher den Schulleitungen und den Lehrkräften Kriterien an die Hand geben, anhand derer datenschutzkonforme Produkte für die Unterrichtsgestaltung erkannt und ausgewählt werden können. Die folgenden Hinweise betreffen zum einen die datenschutzrechtlichen Anforderungen und zum anderen die technischen Mindestanforderungen, auf deren Einhaltung bei der Auswahl in der Praxis zu achten ist.

Internet: https://www.datenschutz-berlin.de
E-Mail: mailbox@datenschutz-berlin.de
Friedrichstr. 219
10969 Berlin
Tel: (030) 13889 - 0
Fax: (030) 13889 201

Aus Datenschutzsicht ist dabei ein besonders wichtiges Kriterium, dass die Lernplattformen nicht mehr personenbezogene Daten erheben und verarbeiten, als für die Unterrichtsgestaltung tatsächlich erforderlich sind.

Uns ist sehr wohl bewusst, dass bei der Dringlichkeit der aktuell zu ergreifenden Maßnahmen für die Aufrechterhaltung des Unterrichtsbetriebs vielleicht nicht alle Anforderungen sofort umgesetzt werden können. Überall dort, wo dies der Fall sein sollte, ist es aber unabdingbar, kontinuierlich nachzubessern. Sollten datenschutzrechtliche Unwägbarkeiten oder gar Missstände auftreten, sind diese umgehend zu beheben. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit wird hier die weitere Entwicklung beobachten und steht auch gern zur Beratung zur Verfügung.

Zum datenschutzrechtlichen Hintergrund:

Die schulrechtlichen Vorschriften im Land Berlin enthalten derzeit keine Regelungen zu den Rahmenbedingungen, unter denen ein Einsatz von Lernplattformen zulässig möglich ist. Seitens der Senatsverwaltung für Bildung, Jugend und Familie wird im Rahmen der Novellierung der Schuldatenverordnung bereits eine entsprechende Vorschrift erarbeitet, mit deren Verabschiedung aber erst mittelfristig zu rechnen ist.

Der Einsatz einer Lernplattform kann daher aktuell nur auf Basis einer freiwillig erteilten Einwilligung der Erziehungsberechtigten und/oder – je nach Alter – der Schülerinnen und Schüler erfolgen. Für die Wirksamkeit dieser Einwilligung sind die Vorgaben des Artikel 7 der Datenschutz-Grundverordnung (DS-GVO) zu beachten.

- Die Einwilligung muss informiert und freiwillig erfolgen. Den Erziehungsberechtigten muss transparent gemacht werden, für welche möglichst genau beschriebenen Zwecke Daten der Schülerinnen und Schüler erhoben und gespeichert werden. Auch muss definiert sein, was mit den Daten geschieht und wie lange diese aufbewahrt werden. Ganz wichtig ist, dass diese Einwilligungserklärung für alle Beteiligten verständlich formuliert ist. Schließlich muss die erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden können.

- Damit die Einwilligung auch tatsächlich freiwillig ist, ist seitens der Schule darauf zu achten, dass auch im Falle einer nicht erteilten Einwilligung die Schülerinnen und Schüler einen alternativen Zugang zu den Materialien erhalten und ihnen so keine Nachteile entstehen.

- Die Schule hat als für die Datenverarbeitung Verantwortliche zu gewährleisten, dass der beauftragte Anbieter die datenschutzrechtlichen Anforderungen erfüllt. Die Schule hat daher festzulegen, welche Daten für die Nutzung der Online-Lernplattform zwingend benötigt werden und muss sicherstellen, dass bei der Lernplattform tatsächlich nur die Daten erhoben und verarbeitet werden, die tatsächlich für die pädagogische Aufgaben der Schule erforderlich sind.

- Bei Nutzung einer Lernplattform eines externen Anbieters muss die Schule als Verantwortliche einen Vertrag über eine Auftragsverarbeitung nach Artikel 28 DS-GVO mit dem Anbieter abschließen. Wichtig ist, dass die Schule als Verantwortliche „Herrin der Daten“

bleibt. Es muss für die Schule als Auftraggeberin ein Weisungsrecht hinsichtlich der Datenverarbeitung beim Dienstleister bestehen. Auch muss die Schule sich vertraglich ein Kontrollrecht einräumen lassen.

- Sofern der Dienstleister Allgemeine Geschäftsbedingungen oder Verträge vorgibt, wie es in der Praxis häufig vorzufinden ist, sind diese gegebenenfalls anzupassen oder zu ergänzen.

- Eine Nutzung der Daten zu eigenen Zwecken des Dienstleisters, beispielsweise zu Forschungszwecken, ist vertraglich auszuschließen oder lediglich aufgrund einer separaten Einwilligung der Erziehungsberechtigten bzw. Schülerinnen und Schüler zu ermöglichen. Eine Ablehnung der Einwilligung darf keine Einschränkung des Dienstes zur Folge haben.

Zu den technischen Mindest-Anforderungen:

Damit eine Online-Lernplattform datenschutzgerecht in Schulen eingesetzt werden kann, müssen die nachstehend aufgeführten technischen Mindestanforderungen erfüllt sein. Auch ist es wichtig, dass gerade bei Angeboten, die die Verarbeitung einer Vielzahl personenbezogener Daten von Schülerinnen und Schülern voraussetzen, ein besonderes Augenmerk auf eine möglichst datensparsame Ausgestaltung gerichtet wird:

- Bei der Einrichtung der Nutzungszugänge muss es möglich sein, pseudonymisierte Zugänge für Schülerinnen und Schüler einzurichten, das heißt, dass diese sich mit einem ausgedachten Namen anmelden können. Die Zuordnung zu dem tatsächlichen Namen der Schülerin bzw. des Schülers darf nicht dem Anbieter der Plattform, sondern nur der unterrichtenden Lehrkraft bekannt sein.

- Die gewählte Online-Lernplattform muss gewährleisten, dass die Lehrerinnen und Lehrer ausschließlich auf die personenbezogenen Daten der von ihnen unterrichteten Schülerinnen und Schüler Zugriff haben. Unberechtigte Dritte, wie zum Beispiel Lehrkräfte, die die Schülerinnen und Schüler aber nicht unterrichten, müssen vom Zugriff auf die gespeicherten Daten ausgeschlossen sein (Mandantenfähigkeit).

- Für die Lernplattform ist ein Löschkonzept erforderlich, welches eine regelmäßige automatische Löschung der Daten nach Schuljahresende vorsieht, wenn nicht Ausnahmen ersichtlich sind, beispielsweise bei schuljahresübergreifenden Projekten. Durch technische Maßnahmen muss sichergestellt sein, dass die Löschung auch entsprechend umgesetzt wird.

- Es ist zu gewährleisten, dass zwischen den Endgeräten der Schülerinnen und Schüler oder denen der Lehrerinnen und Lehrer und dem Server ausschließlich verschlüsselte Verbindungen (TLS 1.2 oder neuer) aufgebaut werden.

- Lokal gespeicherte Daten müssen durch technische und organisatorische Maßnahmen vor dem Zugriff durch Dritte geschützt werden.

- Eingebundene Softwarebibliotheken und genutzte Dienste von Dritten müssen auf ihre datenschutzrechtliche Eignung geprüft werden (welche Daten werden ggf. übermittelt usw.).

- Es muss sichergestellt werden, dass die eingesetzte Software und Softwarebibliotheken aktuell und ohne bekannte Sicherheitslücken sind. Es müssen technische und organisatorische Maßnahmen getroffen werden, die die Software und eventuell vorhandene API-Schnittstellen gegen fehlerhafte Eingaben schützen (beispielsweise durch Web Application Firewalls oder Application Layer Gateways).

Weiterführende Hinweise zu den datenschutzrechtlichen Anforderungen für Online-Lernplattformen finden Sie in der von der Datenschutzkonferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder gemeinsam verabschiedeten „Orientierungshilfe – Online-Lernplattformen im Schulunterricht“ (Stand 26. April 2018), die Sie unter folgenden Link aufrufen können:

https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf