Fragen an LfDI BW vom 23.03.2020 bzgl. Microsoft 365

Sehr geehrte Damen und Herren,

ein Unternehmen, das ich als externer Datenschutzbeauftragter betreue, möchte gerne "Microsoft 365 Business" einsetzen. Bei einer Recherche dazu, ob dieser Einsatz DSGVO-konform möglich ist, bin ich einerseits auf eine Datenschutzfolgeabschätzung der niederländischen Datenschutzaufsichtsbehörde gestoßen, die dies für Microsoft Office 365 Stand 07.11.2018 verneint:

https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office

Seitdem scheint Mircosoft nachgebessert zu haben, allerdings konnte ich durch weitere Recherchen nicht zweifelsfrei ermitteln, ob "Microsoft Office 365" und "Microsoft 365 Business" nun DSGVO-konform sind. Ich habe lediglich diverse Hinweise gefunden, welche Einstellungen in den genannten Produkten vergenommen werden müssen, den Datenschutz zu verbessern. Dass diese Einstellungen jeweils von jedem Anwenderunternehmen vorgenommen werden müssen, ist aber doch ein Verstoß gegen Artikel 25 DSGVO, oder?

Auf Ihren Webseiten habe ich leider auch keine weiteren Informationen gefunden. Es gibt aber in Deutschland einige, insbesondere große Unternehmen, die die genannten Microsoft-Lösungen in der Microsoft-Cloud nutzen. Daher Frage ich mich, wie dies datenschutzrechtlich zu rechtfertigen ist. Könnten Sie mir bitte behilflich sein, so dass ich das von mir betreute Unternehmen die genannten Mircosoft-Lösungen rechtskonform nutzen lassen kann?

Meine zweite Frage geht in eine ähnliche Richtung allerdings diesmal in meiner Rolle als Professor an der Hochschule der Medien in Stuttgart. Aufgrund der Corona-Epidemie und der Verordnung zur Barrierefreiheit, möchten meine Kollegen und ich unsere Lehrmaterialen digital zur Verfügung stellen und dabei die von uns gesprochenen Erläuterungen zu unseren PowerPoint-Folien mittels einer Microsoft Office 365 Cloud-Funktion automatisch mit Untertiteln versehen lassen. Ist diese Nutzung DSGVO-konform? Personenbezogene Daten enthalten unsere Materialien nur dadurch, dass unser Name auf den Folien steht. Allerdings könnte Mircosoft die Nutzungsdaten sämtlicher Studierender auswerten.

Über eine Antwort noch in dieser Woche würde ich mich sehr freuen, da wir mit der Umstellung der Vorlesungsmaterialien auf eLearning-Formate schon jetzt komplett überlastet sind.

Telefonisch bin ich leider bisher nicht durchgekommen, würde dies im Laufe der Woche aber auch notfalls nochmals versuchen.

Mit freundlichen Grüßen

Antwort des LfDI vom 24.03.2020

…

vielen Dank für Ihre Anfrage bzgl. des Einsatzes von Microsoft Office 365.

Allgemein zu Office 365 und zu Ihrer ersten Frage:

Ihre Anfrage kann nicht pauschal beantwortet werden. Zu unterschiedlich sind mögliche nutzende Institutionen, mögliche Verarbeitungszwecke und vor allem die verschiedenen Komponenten, Versionen und Einsatzmodalitäten von Microsoft Office 365.

Microsoft Office 365 ist kein einheitliches Produkt. Es ist ein Sammelname für verschiedene Produkt- und Dienstleistungspakete. Sie unterscheiden sich hinsichtlich der zur Verfügung stehenden Komponenten und zusätzlich (unter anderem) hinsichtlich folgender Aspekte: Manche Varianten werden lokal installiert, andere laufen als „Software as a Service“ online im Browser (z.B. „Office Online“). Möglich ist die Nutzung von Cloud-Speicher für Dokumente usw.; möglich ist aber auch die lokale Speicherung.

Alle Varianten senden standardmäßig sog. „Telemetrie“- und „Diagnosedaten“ an Microsoft, auch das Senden kompletter Speicherabbilder ist möglich.

Nur wenige Enterprise-Varianten ermöglichen es versierten IT-Fachleuten, sehr viele kleinteilige Einstellungen so zu ändern, dass weniger (nicht jedoch keine) dieser Diagnosedaten an Microsoft übermittelt werden. Wenigstens dies zu tun, ist Aufgabe des Verantwortlichen, wobei niemand eine Gewähr dafür bieten kann, dass nach Updates durch Microsoft Einstellungen nicht wieder geändert werden, sodass sich ein rechtswidriger(er) Zustand auch unbemerkt ergeben kann. Uns ist derzeit keine einfach zu übernehmende Konfiguration bekannt, die alle Datenflüsse abschaltet. Eine Einwilligung der betroffenen Mitarbeiter im Beschäftigungsverhältnis in die Weitergabe von Nutzungsdaten an Microsoft scheidet wegen des klaren Ungleichgewichts zwischen Arbeitgeber und Mitarbeiter aus (vgl. Erwägungsgrund 43 der Datenschutzgrundverordnung – DS-GVO).

Wer diese Software betreibt und die Dienste nutzt, dürfte alleine oder gemeinsam (Art. 26 DS-GVO) mit Microsoft für die damit verbundenen Datenflüsse verantwortlich sein. Dass eine Rechtsgrundlage diese oder die bei Microsoft nachfolgende Verarbeitung erlaubt, ist nicht ersichtlich. Auch wenn Microsoft für die Verarbeitung verantwortlich ist, bedarf es einer Rechtsgrundlage für die Übermittlung der Daten an Microsoft. Ggf. ist der Betriebsrat einzubeziehen.

Die vielen Komponenten bieten viele Funktionalitäten. Sie jeweils einzusetzen, bedarf der vorherigen Prüfung durch den Verantwortlichen im Hinblick auf das Vorhandensein einer einschlägigen Rechtsgrundlage für den jeweiligen Zweck, die jeweilige Verarbeitung, die technischen und organisatorischen Maßnahmen zum Schutz der Daten usw.

Soweit es sich hier um eine Verarbeitung im Auftrag handelt, muss das Unternehmen als verantwortliche Stelle Artikel 28 DS-GVO beachten, so dass die Verarbeitung im Einklang mit der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet ist. Dabei darf das

Unternehmen als verantwortliche Stelle nur solche Auftragsverarbeiter auswählen, welche die Anforderungen der DS-GVO gewährleisten können.

Bei der Auswahl einer Software oder eines Dienstes ist deswegen u.a. zu prüfen, ob alle datenschutzrechtlichen Vorgaben umgesetzt werden und unerwünschte Datenübertragungen einschließlich Auswertung des Nutzerverhaltens erfolgen, damit die Rechtmäßigkeit der Verarbeitung sichergestellt ist. Dies betrifft im Falle von Office 365 nicht nur die angesprochen Diagnose- und Telemetriedaten, sondern auch Nutzungsdaten im Zusammenhang mit dem Office-Graph und MyAnalytics. Sollte diese Prüfung nicht möglich sein, z.B. weil nicht alle Datenflüsse und Verarbeitungen vom Hersteller ausreichend dokumentiert sind, kann eine solche Software nicht datenschutzkonform eingesetzt werden, schon weil die Datenverarbeitung nicht den Grundsätzen für die Verarbeitung personenbezogener Daten (vgl. Artikel 5 DS-GVO) entspricht. Nach Artikel 5 Absatz 2 DS-GVO ist das Unternehmen hierfür rechenschaftspflichtig. Dabei sind nicht nur die angezeigten Daten zu prüfen, sondern auch, welche ohne Anzeige gespeichert, übertragen und verarbeitet werden.

Ebenso ist Kapitel V der DS-GVO (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen) zu beachten.

Im Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DS-GVO muss das Unternehmen als verantwortliche Stelle die entsprechenden Überlegungen dokumentieren.

Sollte bei der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bestehen, müsste weiterhin eine Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO vorgenommen werden. Ein hohes Risiko besteht z.B. bei der Verarbeitung von besonderen Kategorien personenbezogener Daten nach Artikel 9 DS-GVO, also z.B. bei Gesundheitsdaten (auch Krankmeldungen), Daten über die politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die sexuelle Orientierung.

Eventuell liegt auch eine gemeinsame Verantwortung bei der Verarbeitung der Daten nach Artikel 26 DS-GVO vor. Entsprechende Vereinbarungen sind hierfür zu erstellen und es ist zu klären, welche Rechtsgrundlage eine dann vorliegende Übermittlung von personenbezogenen Daten von dem Unternehmen an Microsoft datenschutzrechtlich legalisiert. Hierzu sind nicht nur die im Cloud-Dienst gespeicherten Dokumente, sondern auch weiteres wie sog. Telemetrie- und Diagnosedaten zu betrachten.

Wir sind in Zusammenarbeit mit den Aufsichtsbehörden der anderen Länder seit längerem mit Microsoft in Kontakt um die angesprochenen Fragen zu besprechen, allerdings konnten noch nicht alle unsere Fragen endgültig geklärt werden.

Bei US-amerikanischen Anbietern ist noch eine Besonderheit zu beachten: Diese Anbieter sind auch bei Rechenzentren, die im europäischen Wirtschaftsraum liegen, der Gesetzeslage in ihrem Heimatland verpflichtet. Dies bedeutet im konkreten Fall, dass Daten aus diesen Rechenzentren US-Sicherheitsbehörden zugänglich gemacht werden können.

Unsere Dienststelle entwickelt derzeit eine Hilfestellung für Verantwortliche zur eigenverantwortlichen Prüfung von Cloud-Diensten. Sobald diese erscheint, kann sie auch zur Bewertung des rechtskonformen Einsatzes einer Software in der gewählten Konfiguration und Variante eingesetzt werden.

Zu Ihrer zweiten Frage:

Zusätzlich zu den obigen Ausführungen beachten Sie bitte, dass bei der automatischen Transkribierung für die Erstellung der Untertitel die Aufnahmen von den Anbietern (in diesem Falle also Microsoft) in der Regel auch für eigene Zwecke ausgewertet, gespeichert und oftmals auch abgehört werden. bzgl. der digitalen Zurverfügungstellung der Lehrmaterialen beachten Sie bitte auch die obigen Ausführungen auf Frage 1.

Welche Daten Microsoft bei der Nutzung von Office 365 durch die Studenten verarbeitet ist uns nicht bekannt und hängt auch von der konkreten Konfiguration ab. Diese Verarbeitung bedarf aber einer eigenen Rechtsgrundlage und ggf. Abschluss eines Auftragsverarbeitungsvertrages oder eines Vertrages über die gemeinsame Verantwortlichkeit. In manchen Regelungsbereichen ist Auftragsverarbeitung, gerade auch solche durch öffentliche Stellen, nur eingeschränkt (z.B. § 80 des Zehnten Buches Sozialgesetzbuch, § 85a des Landesbeamtengesetzes) oder ggf. gar nicht erlaubt. Für den Unterricht kann anderes gelten als für Verwaltungsaufgaben.

Daher empfehlen wir, die fertigen Lehrmaterialien auf der Website der Hochschule den Studierenden bereit zu stellen. Damit sind keine Dritten involviert, erhalten keine Informationen über das Nutzungsverhalten der Studenten und Sie bzw. die Hochschule erspart sich den Aufwand für die tiefergehende datenschutzrechtliche Prüfung.