Microsoft 365 in Kirche & Wohlfahrt

Orientierungshilfe Datenschutz und IT-Sicherheit
zu Einführung und Einsatz von Microsoft 365
nach DSGVO sowie KDG, KDR-OG und DSG-EKD

Version 2.1

Stand: 09.01.2023

ALTHAMMER & KILL
SoCura

Microsoft 365 in Kirche & Wohlfahrt

Orientierungshilfe Datenschutz und IT-Sicherheit zu Einführung und Einsatz von Microsoft 365 nach DSGVO sowie KDG, KDR-OG und DSG-EKD

Version 2.1

Herausgeber/Autoren:

Althammer & Kill GmbH & Co. KG, Hannover (info@althammer-kill.de)
Simon Lang, Thomas Althammer

SoCura gGmbH, Köln (info@socura.de)
Philip Huefnagels-Vajda, Dr. Karsten C. Ronnenberg

Die Microsoft Lizenz- und Vertragsmodelle sind vielfältig. Auf den folgenden Seiten wird von einem Zugang zum „Enterprise Agreement“ ausgegangen, für das es Vertragsanlagen zum DSG-EKD oder § 203 StGB gibt. Andere Lizenzformen, insbesondere aus dem Consumer und SME-Bereich wurden nicht betrachtet.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern meist die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Informationen zur 2. Auflage

Sehr geehrte Leserin, sehr geehrter Leser,

wir freuen uns Ihnen die zweite Version der Orientierungshilfe „Microsoft 365 in Kirche & Wohlfahrt“ präsentieren zu dürfen. Gegenüber der ersten Fassung haben wir folgende Änderungen und Neuerungen aufgenommen:

- Neustrukturierung der Kapitel, angelehnt an den Lebenszyklus von Microsoft 365 sowie Vorüberlegungen und Managemententscheidungen bei Einführung von Microsoft 365
- Rechtliche Neuerungen: u. a. neue Standarddatenschutzklauseln, Transfer Impact Assessment, Videosprechstunde und Telemedizin, Abgleich mit neuen Gesetzen aus den Bereichen Telekomunikation und Telemedien.
- Überarbeitung und Ergänzung relevanter technischer Informationen, insbesondere zu Verschlüsselungsverfahren
- Analysen zu internationalen Datenströmen und Verarbeitungs-/Speicherorten

Weiterhin sprechen wir teils von Microsoft 365, teils von Office 365. Streng genommen handelt es sich um zwei verschiedene Angebote und unterschiedliche „Pläne“, wobei Office 365 in Microsoft 365 enthalten ist. Die Aussagen werden zumeist auf beide Angebotsformen zutreffen.

Das Autoren-Team, im Sommer 2022

Einleitung

Organisationen in Kirche & Wohlfahrt stehen vor einem Dilemma: Während der Pandemie musste „mobiles Arbeiten“ in kürzester Zeit eingeführt werden. Wo noch vor Jahren der ausschließliche Zugriff aus dem Unternehmensnetzwerk erfolgte, findet sich heute als Anforderung ein Arbeiten von überall auch im Gesundheits- und Sozialwesen. Die Microsoft 365-Welt steht auf Knopfdruck über alle möglichen Geräte jederzeit zur Verfügung.

Gleichzeitig sind die Aufsichtsbehörden in Sachen Datenschutz bei Cloud-Diensten mit außereuropäischen Wurzeln aufgrund der aktuellen Rechtslage sehr kritisch eingestellt. Zu viele Fragen sind noch nicht geklärt Aufgrund der „Schrems II“-Thematik gibt es große Vorbehalte gegen den Einsatz von Microsoft 365 und vergleichbarer Dienste.

Die Lösung des gordischen Knotens werden wir – Stand Sommer 2022 – weiterhin nicht präsentieren können. Gleichwohl haben wir Verständnis für beide Lager. Der Einsatz von Microsoft Cloud-Lösungen ist nicht immer technisch und rechtlich bedenkenlos möglich. Die Entscheidung muss am Ende des Tages jede Organisation bezogen auf die eigenen Anforderungen und den gewünschten Nutzungsumfang für sich selbst beantworten.

Warum dann dieses Whitepaper in der nun vorliegenden überarbeiteten Fassung? Die Autoren der Beratungshäuser SoCura sowie Althammer & Kill verfügen jeweils über eine gewachsene Expertise in der rechtlichen und technischen Beratung bei der Einführung von Microsoft Cloud-Lösungen (nachfolgend gemeinschaftlich „M365“) für Rechtsträger im Bereich Kirche & Wohlfahrt. Die Autoren möchten wesentliche Erkenntnisse mittels der vorliegenden Orientierungshilfe anhand einiger Leitfragen an Interessierte weitergeben.

Organisationen im Bereich Kirche & Wohlfahrt setzen sich zunehmend mit der Digitalisierung auseinander. Nicht nur bedingt durch die Pandemie ist die Kommunikation mittels Chats und Videokonferenzen zum Standard geworden. Innerhalb weniger Monate haben sich neue Formen der Zusammenarbeit etabliert, die aus unserem Berufsalltag nicht mehr wegzudenken sind.

In Hinblick auf die (IT-)Governance wandelt sich das Bild durch kollaboratives Arbeiten. Im Umgang mit modernen Kommunikations- und Arbeitsmitteln wird an vielen Stellen nicht mehr nur das „Need-to-Know“-Prinzip, sondern auch das „Need-to-Protect“-Prinzip[1] gelten.

Zugleich hat sich mit dem zielgerichteten „Teilen“ von Dokumenten die Notwendigkeit zum Umdenken bei der Gestaltung von Arbeitsprozessen und Berechtigungskonzepten entwickelt. Dateien werden mit modernen Cloud-Lösungen kollaborativ entwickelt. Ein Austausch von Bearbeitungsständen per E-Mail ist unpraktisch und fehleranfällig. Punktuell geteilte Dateien oder Ordner ersetzen enge Zugriffsrechte an Abteilungsgrenzen.

Das bringt Verantwortliche in Zugzwang: Auf der einen Seite müssen Weichen weiter in Richtung Digitalisierung gestellt werden. Das erfolgt nicht zuletzt, um in Krisenzeiten handlungsfähig zu bleiben. Ein wichtiger Entscheidungsfaktor hierbei sind die (Implementierungs-)Kosten und die Schwierigkeit, Abhängigkeit und Rechtsunsicherheit genauer zu beziffern.

Die Entscheidung über den Einsatz von M365 als ein solches modernes Kommunikations- und Arbeitsmittel andererseits stellt eine Organisation jedoch bereits im Kontext der Datenschutz-Grundverordnung (DSGVO) vor viele Fragen und Herausforderungen.

[1] Bei Need-to-Know geht es um die Eingrenzung, welcher Personenkreis von Informationen Kenntnis haben muss. Bei Need-to-Protect werden Informationen bspw. der gesamten Organisation zur Verfügung gestellt. Die Grenze bildet dabei die Erfüllung der Compliance.

Im weltlichen Bereich ist DSGVO-Konformität ein wesentliches Kriterium bei der Auswahl von Cloud-Lösungen. Dies gilt im Bereich Kirche & Wohlfahrt umso mehr, da die Vorgaben der kirchlichen Aufsichtsbehörden teilweise über die der weltlichen Behörden hinausgehen und zudem im Kontext des kirchlichen Datenschutzes u. a. nicht in der Breite auf Gesetzeskommentare, Rechtsprechung und Entscheidungshilfen zurückgegriffen werden kann. Zudem verarbeiten Organisationen aus Kirche & Wohlfahrt zumeist Sozial- und Gesundheitsdaten, die als besonders schützenswert eingestuft werden.

Wie ist dieses Dilemma zu lösen? Die folgende Abbildung zeigt – stark vereinfacht – mögliche Strategien im Umgang mit den technischen und rechtlichen Entwicklungen auf, die im Kontext der eigenen Organisation bewertet und diskutiert werden wollen. Die dargestellten Wege und Handlungspfade sind stark vereinfacht und lassen sich in viele weitere feine Abstufungen unterteilen.

Nach der anfänglichen Euphorie über erreichte große Schritte in Sachen Digitalisierung ist in vielen Organisationen Ernüchterung und Verunsicherung eingetreten. Wie ist die IT-Strategie im Lichte der rechtlichen Unsicherheiten und verfügbaren Marktangebote weiter zu gestalten? Welche Risiken und Abhängigkeiten bergen der Einsatz moderner Kollaborationswerkzeuge?

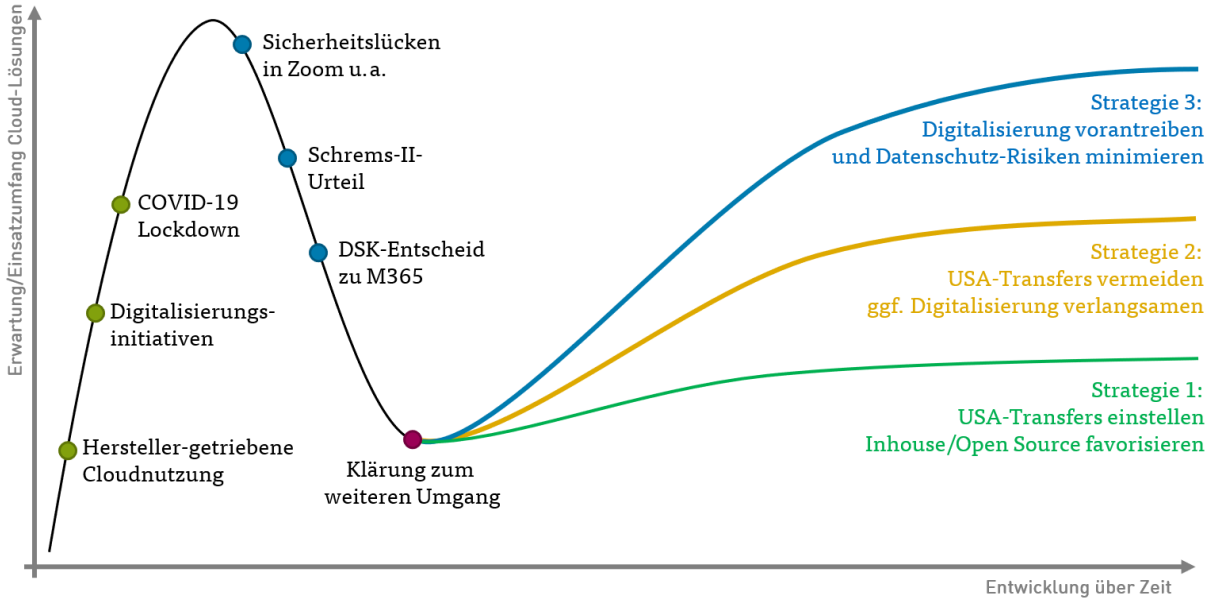


Abbildung 1: Digitalisierungsstrategien im Kontext von Cloud-Nutzung und IT-Compliance-Fragen[2]

Mit dem vorliegenden Papier in der überarbeiteten Fassung sollen aktuelle und wiederkehrende Fragen rund um die Einführung und den Einsatz von M365 bei Rechtsträgern aus Kirche & Wohlfahrt aufgegriffen werden. Das Papier stellt einerseits eine Orientierungshilfe dar und zeigt auf der anderen Seite gesetzliche und technische Regelungslücken auf, die es mit Gesetzgeber, Aufsichtsbehörden und auch Microsoft zu diskutieren gilt.

Verantwortlich für die folgenden Darstellungen sind ausnahmslos die Autoren von Althammer & Kill bzw. der SoCura. Nach Fertigstellung wurde das Whitepaper vorab an verschiedene Experten (siehe Anhang) zur kritischen Durchsicht vorgelegt, deren Feedback in der Orientierungshilfe (Version 1) berücksichtigt worden ist.

[2] vereinfachte Darstellung aus Management-Workshop IT-Strategie, Cloud und IT-Compliance (Quelle: Althammer & Kill)

I. Vorüberlegungen und Managemententscheidungen

Ganz unabhängig davon, um welche Technologie es geht: Die Einführung von neuen Technologien erfolgt, um einen Geschäftszweck zu erreichen. In der Regel definieren Organisationen vorab einen solchen als Mission, sowie davon abgeleitete Geschäftsziele (Business Goals), die in Form von Initiativen (Initiatives) erreicht werden sollen. Dazu werden Projekte aufgesetzt, die auf eine oder mehrere Initiativen einzahlen und sich unterschiedlicher Hilfsmittel (z. B. Software-Lösungen) bedienen.

Einführung oder Transformation von Technologie erfolgen häufig entlang typischer Phasen. Im Kontext M365 ist die Auswahl und Bewertung besonders anspruchsvoll, da sich viele Organisationen erstmalig mit der Nutzung von Public Cloud-Diensten beschäftigen.

Vorbereitung

Im ersten Schritt muss analysiert werden, ob die Nutzung einer neuen Software oder – im Kontext M365 – die Verlagerung von Verarbeitungsprozessen in die Cloud im Sinne der Organisationsziele ist. Denn es ist klar, dass mit der Einführung von M365 nicht unerhebliche Teile der IT-Infrastruktur in eine Cloudumgebung ausgelagert werden und somit nicht mehr dem direkten und alleinigen Zugriff der eigenen Organisation unterliegen. Dazu gilt es unabhängig von datenschutzrechtlichen Fragestellungen Chancen und Risiken sorgfältig abzuwägen.

Weiterhin bedeutet die Auslagerung von bestimmten Diensten und Services in eine gemanagte Cloudumgebung wie M365 nicht automatisch, dass innerhalb der eigenen Organisationen keine Know-How-Träger mehr für diese Dienste und Services benötigt werden. Auch die eigene M365 Umgebung will verwaltet und administriert werden. Dafür ist qualifiziertes Personal erforderlich, dass die Spezifika und Konfigurationsmöglichkeiten der einzelnen Dienste beherrscht.

Evaluierung

An die Stelle klassischer Lizenzmodelle und Lizenzverträge sind Abonnements und „Pläne“ getreten. Während im Einstieg nur die klassischen Office-Anwendungen wie Word und Excel enthalten sind, umfassen die meisten Business- und Enterprise-Pläne zusätzliche Produkte wie Exchange, SharePoint und OneDrive.

Zunächst ist also herauszufinden, welche „Pläne“ operativ und strategisch sinnvoll zu meiner Organisation und den angedachten Einsatzzweck passen. Microsoft versteht es hervorragend, eine fast unüberschaubare Auswahl an unterschiedlichen Einzelplänen und/oder Lizenzpaketen anzubieten und damit die Auswahl der ressourcenschonendsten Variante zu einer Herkulesaufgabe werden zu lassen.

Datenschutz und Datensicherheit

Welche Daten sollen innerhalb von M365 verarbeitet werden? Danach richtet sich die Wahl der Authentifizierung, der Verschlüsselung sowie Einsatzbedarf von Data Loss- und Threat-Prevention. Begleitend müssen die zu erwartenden Nutzungsszenarien in die Überlegungen einfließen: Erfolgt die Arbeit aus einen geschützten Corporate Network mit dienstlich administrierten Geräten oder auch mittels privater Hardware „von überall“? Welche Rollen spielen externe Kooperationspartner?

Viele Organisationen in Kirche und Wohlfahrt arbeiten mit einer großen Zahl von Ehrenamtlichen zusammen. Wie sind diese in die IT-Umgebung und den Einsatz von M365 einzubinden?

Ganz entscheidend im kirchlichen Kontext muss im Bewusstsein von Vorstand und Geschäftsführung sein, dass die Einführung von M365 letztlich eine Entscheidung auf Managementebene ist. Risiken und Verantwortlichkeiten können von der „verantwortlichen Stelle“ nicht auf einen technischen Dienstleister oder Microsoft abgewälzt werden. Bei einer Entscheidung zugunsten M365 ist eine Untersagung durch Aufsichtsbehörden als datenschutzrechtliches Risiko zu akzeptieren.

Lifecycle-Management

Zu guter Letzt spielt das Lifecycle-Management eine große Rolle, da die Dienste und Services kontinuierlich und vor allem autark durch Microsoft „verändert“ werden. Sie haben nicht mehr die Möglichkeit, funktionale Anpassungen durch das „Auslassen“ von Updates zu verzögern.

Als Organisation muss man somit kontinuierlich am „Zahn der Zeit“ des Providers bleiben, bevorstehende Änderungen prüfen und mit den eigenen Anforderungen abgleichen, um im Zweifelsfall rechtzeitig gegensteuern zu können: Sei es durch Umlizenzierung, da sich Pakete und deren Inhalte ändern oder gar eine Verlagerung bestimmter Dienste und Services auf einen anderen Provider.

Geänderte und neue Funktionen werden automatisch eingespielt und können vorhandene Datenschutz- und Sicherheitseinstellungen unterlaufen. Immer wieder konnten wir in den letzten Jahren beobachten, dass Neuerungen in M365 automatisch eingespielt wurden, ohne vorab zu fragen, ob das auch von der Organisation gewünscht war. Es ist also laufend zu prüfen, ob die vielen Updates und Neuerungen datenschutzrechtlich und Compliance-technisch erwünscht sind oder ob hier kurzfristig nachjustiert werden muss, z. B. mit Abschalten von Diensten oder der Anpassung der Datenschutzdokumentation.

II. Arbeiten mit Microsoft 365

Dürfen sensible Daten in der Cloud gespeichert werden? Können oder müssen Dateien zusätzlich geschützt werden?

Für die Speicherung sensibler Daten sollten zusätzliche Sicherungsmaßnahmen (bspw. Verschlüsselung) getroffen werden. Zum einen können Anwender selbst in M365 entsprechende Maßnahmen vornehmen, zum anderen stehen der Organisation hier verschiedene Möglichkeiten offen.

Was bezeichnet „sensible Daten“?

Es liegt im Wesen von Kirche und Wohlfahrt, dass regelmäßig sensible Daten verarbeitet werden – etwa Patientendaten in Pflege und Hospiz oder die Daten von Geflüchteten. Was sensible Daten angeht, die einen Personenbezug aufweisen, sind die sogenannten „besonderen Kategorien personenbezogener Daten“ fest im Datenschutzrecht umrissen:

> *„[…] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person […]“.*[3]

Der kirchliche Datenschutz folgt hierin weitgehend dem EU-Recht, nimmt jedoch die bloße Angabe über die Zugehörigkeit einer Person zu einer Kirche oder einer Religionsgemeinschaft von der Definition aus.[4] Dass jemand katholisch oder evangelisch ist, ist also nach kirchlichem Recht kein besonders schützenswertes Datum.

Über den Datenschutz im engeren Sinne hinaus gibt es Daten, die einer besonderen Schweigepflicht unterliegen, bspw. Einem Berufsgeheimnis[5], dem Fernmeldegeheimnis[6] oder dem Sozialgeheimnis[7]. Darüber hinaus kann es vertraglich vereinbarte Geheimhaltungspflichten geben.

Daten können zudem aufgrund ihres wirtschaftlichen oder operativen Wertes sensibel für eine Organisation sein. Die entsprechenden Dokumente werden dann als geheimhaltungsbedürftig eingestuft. Hier ist das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) anwendbar, das jedoch keine Vorgaben zur praktischen Einstufung von Informationen macht.[8] Ein System zur Klassifizierung von Dokumenten, bspw. Nach öffentlich, intern, vertraulich und ggf. streng vertraulich, muss eine Organisation selbst implementieren.

In den kommenden Jahren ist mit weiteren Gesetzen und Verordnungen im Kontext Daten zu rechnen. Die EU will den Umgang mit Daten revolutionieren und zum Vorbild für einen modernen „Datenmarkt“ bzw. eine „Datenwirtschaft“ werden.[9]

---

[3] Art. 9 Abs. 1 DSGVO.
[4] § 4 Nr. 2 KDG / § 4 Nr. 2 DSG-EKD.
[5] § 203 StGB.
[6] § 88 TKG.
[7] § 78 Abs. 1 Satz 2 & 3 SGB X.
[8] Nach jüngster Rechtsprechung können angemessene Geheimhaltungsmaßnahmen auch in vertraglichen Vereinbarungen liegen; vgl. LAG Düsseldorf, Urteil vom 03.06.2020 - 12 SaGa 4/20.
[9] vgl. europäische Gesetzesvorhaben zum „Digital Markets Act“, „Digital Services Act“, „Data Governance Act“ und „Data Act“

Welche Anforderungen werden an die Speicherung sensibler Daten gestellt?

Aus der Einstufung von Daten als „sensibel“ ergeben sich höhere Anforderungen an die Sicherheit der Speicherung und Verarbeitung. Sensible Daten sind stets mit höheren Risiken verbunden, da eine Verletzung der Schutzziele von Vertraulichkeit, Integrität oder Verfügbarkeit größere Auswirkungen haben können. Dementsprechend ist ihr Schutzbedarf als höher anzusehen.[10]

Besonderheiten im KDG

Nach der „Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz“ (KDG-DVO)[11] dürfen sensible Daten nur verschlüsselt abgespeichert werden und die langfristige Lesbarkeit der Daten muss sichergestellt werden. Zudem muss ein Datensicherungskonzept erstellt werden.[12]

Besonderheiten im DSG-EKD

Der BfD EKD setzt bei Nutzung von Cloud-Diensten eine verschlüsselte Speicherung von besonderen Kategorien personenbezogener Daten voraus, selbst wenn diese im europäischen Wirtschaftsraum verarbeitet werden.[13]

Können oder müssen Dateien durch Anwender zusätzlich geschützt werden?

M365 bietet nach Einschätzung der Autoren ein hohes Maß an Sicherheit durch Technik und durch Voreinstellungen, die von Systemadministratoren vorgenommen werden können. Mithilfe von Data Loss Prevention (DLP) oder der Klassifizierung von Inhalten können weitreichende Informationen zum Schutzbedarf mitgegeben und auf Basis von Regeln überprüft werden. Die M365-Dienste bieten hier mit Bordmitteln bereits weitreichendere Möglichkeiten, als das im On-Premise-Umfeld bisher möglich war. Die Schutzmaßnahmen können sowohl auf Ebene der Dateien selbst als auch für Speicherorte angewandt werden.

Bei den Anwenderinnen und Anwendern ist es erforderlich, für das nötige Bewusstsein über einen erhöhten Schutzbedarf zu sorgen und Kenntnisse über Möglichkeiten der Dienste zu schaffen, um den Schutz der Daten aktiv zu gewährleisten – sowohl gegenüber Externen als auch gegenüber Mitgliedern der eigenen Organisation.

[10] Vgl. Art. 32 Abs. 2 DSGVO, § 22 Abs. 2 BDSG / § 26 Abs. 2 KDG / § 27 Abs. 2 DSG-EKD.
[11] §§ 9-14, 25 KDG-DVO.
[12] § 13 Abs. 2; § 16 KDG-DVO. Für Daten, die dem Beicht- oder Seelsorgegeheimnis nach kanonischem Recht unterliegen, sind eigene Anforderungen definiert; vgl. § 14 KDG-DVO.
[13] https://datenschutz.ekd.de/wp-content/uploads/2021/10/GemeinsameStellungnahmeDatenuebermittlungUSA.pdf (zuletzt abgerufen am 12.09.2022)

Formen der Verschlüsselung und wie diese aktiviert werden (HYOK/BYOK)

Microsoft bietet verschiedene Verschlüsselungsmethoden im M365-Umfeld an, u. a. Bring Your Own Key (BYOK), Hold Your Own Key (HYOK) und Double Key Encryption (DKE).

Generelles zur Verschlüsselung

Durch einen Verschlüsselungsprozess werden Daten im Klartext mit Hilfe eines geheim zu haltenden Schlüssels in einen Geheimtext umgewandelt; der zugehörige Klartext kann nur unter Verwendung des (geheimen) Schlüssels rekonstruiert werden. Durch die Verschlüsselung wird so das Schutzziel der Vertraulichkeit realisiert, da nur autorisierte Empfänger – also diejenigen, die einen berechtigten Zugriff auf den geheimen Schlüssel haben – die Inhalte entschlüsseln können.

Die Verschlüsselung muss Teil einer umfassenderen Informationssicherheitsmanagement-Strategie für die gesamte Organisation sein, denn mithilfe der Verschlüsselung wird ein Abhören der Daten nicht grundsätzlich verhindert. Jedoch wird sichergestellt, dass nur autorisierte Personen die verschlüsselten Daten entschlüsseln können.

Verschlüsselung kann auf mehreren Ebenen gleichzeitig eingesetzt werden. Beispielsweise können sowohl die E-Mail-Nachrichten selbst als auch der bei der E-Mail-Kommunikation verwendete Kommunikationskanal verschlüsselt werden. Mit M365 werden sowohl gespeicherte Daten (engl.: „data at rest“, frei übersetzt: „Daten im Ruhezustand“) als auch die (noch) in der Übertragung befindlichen Daten (engl.: „data in transit“, frei übersetzt: „Daten beim Transport“) verschlüsselt, wobei gängige Verschlüsselungsprotokolle und Technologien zum Einsatz kommen. Dies sind auf Transportebene u. a. die „Transport Layer Security (TLS)“, auf IP-Ebene die „Internet Protocol Security (IPSec)“ und als eigentliches Verschlüsselungsverfahren Bspw. der „Advanced Encryption Standard (AES)“.[14]

Verschlüsselung von Daten im Ruhezustand ("data at rest“) und während der Übertragung („data in transit“)

Nachfolgende Tabelle zeigt die Verschlüsselungsmethoden in Microsoft 365 auf, so wie Microsoft sie selbst darstellt.

Arten von Inhalten	**Verschlüsselungstechnologien**
Dateien auf einem Speichermedium, z. B.: - E-Mail-Nachrichten, die in einem Ordner gespeichert sind, - Office-Dokumente, die auf einem Computer, Tablet oder Smartphone gespeichert sind, - Daten, die in der Microsoft Cloud gespeichert sind	**BitLocker** in Microsoft-Datencentern. BitLocker kann auch auf Clientcomputern verwendet werden, wie Windows-Computer und Tablets. **Distributed Key Manager (DKM)** in Microsoft-Rechenzentren Kundenschlüssel für Microsoft 365
Dateien während der Übertragung zwischen Benutzern, z. B.:	**TLS** für Dateien während der Übertragung

[14] Siehe hierzu und im Folgenden https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption?view=o365-worldwide, zuletzt abgerufen am 14.07.2022

Arten von Inhalten	Verschlüsselungstechnologien
- Office-Dokumente - SharePoint-Listenelemente, die von Benutzern gemeinsam verwendet werden	
E-Mails während der Übertragung zwischen Empfängern (gehostet von Exchange Online)	Office-365-Nachrichtenverschlüsselung mit **Azure Rights Management**, **S/MIME** und **TLS** für E-Mails während der Übertragung
Chats, Nachrichten und Dateien während der Übertragung zwischen Empfängern mithilfe von Microsoft Teams	Microsoft Teams verwendet **TLS** und **MTLS** zum Verschlüsseln von Chatnachrichten. Der Mediendatenverkehr wird mithilfe von SRTP (Secure RTP) verschlüsselt. Microsoft Teams verwendet FIPS (Federal Information Processing Standard)

Mit Office 365 arbeiten mehrere Ebenen und Verschlüsselungstypen zusammen, um die Daten zu schützen. Die nachfolgende Auflistung enthält Informationen zur Azure Information Protection.

Hinweis: Azure Information Protection ist nur in bestimmten Microsoft 365-Lizenzvarianten verfügbar[15]. ([16]):

	Microsoft 365 Apps for Enterprise Jetzt für 12,80 € Benutzer/Monat kaufen (Jahresabonnement mit automatischer Verlängerung)	Office 365 E1 Jetzt für 8,40 € Benutzer/Monat kaufen (Jahresabonnement mit automatischer Verlängerung)	Office 365 E3 Jetzt für 22,60 € Benutzer/Monat kaufen (Jahresabonnement mit automatischer Verlängerung)	Office 365 E5 Jetzt für 37,40 € Benutzer/Monat kaufen (Jahresabonnement mit automatischer Verlängerung)
Informationsschutz Vertrauliche Daten an nahezu jedem Ort schützen, auch bei der Übertragung und Freigabe – plus Transparenz und Kontrolle über die Nutzung jeder einzelnen Datei in einer integrierten Lösung			✓	✓
Informationsschutz – Nachrichtenverschlüsselung, Rechteverwaltung, Verhinderung von Datenverlust für E-Mails und Dateien			✓	✓
Azure Information Protection			✓	✓
Office 365 Cloud App Security				✓

Von Microsoft generierte Mandantenstammschlüssel (Cloud-basiert)

Der Standardschlüssel wird automatisch von Microsoft generiert. Dieser sollte nur in Testumgebungen zum Einsatz kommen oder von Organisationen genutzt werden, die keinen gesetzlichen Vorschriften bzgl. des Schlüsselmanagements unterliegen.

[15] Siehe https://m365maps.com/matrix.htm (zuletzt abgerufen am 12.09.2022)
[16] Siehe https://www.microsoft.com/de-de/microsoft-365/enterprise/compare-office-365-plans?market=de (zuletzt abgerufen am 12.09.2022)

Bring Your Own Key (BYOK) (Cloud-basiert)

Neben dem von Microsoft generierten Schlüssel ist es ebenfalls möglich, einen eigenen Schlüssel mitzubringen („Bring Your Own Key", kurz BYOK) bzw. zu generieren. Zu den Anwendungen, die dieses Vorgehen unterstützen, gehören:

- Cloud-Dienste wie Microsoft SharePoint oder Office 365
- Lokale Dienste, die Exchange- und SharePoint-Anwendungen ausführen, die den Azure-Rights-Management-Dienst über den RMS-Connector verwenden
- Client-Anwendungen, z. B. Office 2019, Office 2016 und Office 2013

Von Organisationen generierte Schlüssel (BYOK) werden in Azure Key Vault[17] gespeichert (im Gegensatz zur HYOK-Konfiguration). Azure Key Vault ist eine Cloud-basierte Schlüsselverwaltungslösung.[18]

Double Key Encryption (DKE)

Bei der Double Key Encryption werden zwei Schlüssel zusammen verwendet, um auf geschützte Inhalte zuzugreifen. Microsoft speichert einen Schlüssel in Microsoft Azure, die Organisation den anderen Schlüssel. Diese Art der Verschlüsselung ist besonders empfehlenswert, wenn

- sichergestellt werden soll, dass Microsoft keine Zugriffsmöglichkeiten auf die Daten haben soll und/oder
- regulatorische Anforderungen dazu verpflichten, den Schlüssel innerhalb eines geografischen Gebietes zu halten.

Hinweis: Double Key Encryption ist nur in bestimmten Lizenzmodellen verfügbar.[19]

Hold Your Own Key (HYOK)

Mit Azure Information Protection ist es möglich, eine „Hold Your Own Key"-Konfiguration vorzunehmen, kurz HYOK. HYOK verwendet einen zusätzlichen, vom Kunden gehaltenen Schlüssel, der lokal für hochsensible Inhalte gespeichert und verwendet wird.[20] Dieses Verschlüsselungsverfahren eignet sich besonders für Organisationen, die besonderen gesetzlichen Vorschriften unterliegen und die getrennte Haltung des Schlüssels der Cloud-Umgebung zur Voraussetzung machen.

Die Isolation bedeutet, dass verschlüsselte Inhalte nur von lokalen Anwendungen und lokalen Diensten gelesen werden können. Anleitungen zur Implementierung von BYOK und HYOK sind bei Microsoft abrufbar.[21]

---

[17] Die Verwendung von HSM-geschützten Schlüsseln in der Azure Key Vault erfordert eine Azure Key Vault Premium-Dienst Ebene, die eine zusätzliche monatliche Abonnementgebühr verursacht

[18] Weitere Informationen zu Azure Key Vault sind unter folgendem Link abrufbar: https://azure.microsoft.com/de-de/services/key-vault/

[19] Siehe https://m365maps.com/matrix.htm, zuletzt abgerufen am 08.03.2022

[20] Siehe hierzu und im Folgenden https://docs.microsoft.com/de-de/azure/information-protection/configure-adrms-restrictions, zuletzt abgerufen am 08.03.2022

[21] BYOK: https://docs.microsoft.com/de-de/azure/information-protection/byok-price-restrictions, zuletzt abgerufen m 14.07.2022
HYOK: https://docs.microsoft.com/de-de/azure/information-protection/configure-adrms-restrictions, zuletzt abgerufen am 14.07.2022

Cloud-basierter Schutz im Vergleich zu DKE und HYOK

Cloud-basierter Schutz eignet sich insbesondere für sensible Dokumente, die jedoch nicht mit der HYOK-Methode geschützt werden müssen. Die Azure Information Protection verwendet hierzu einen Cloud-basierten Schlüssel, der entweder von Microsoft oder vom Kunden selbst mithilfe der BYOK-Konfiguration (siehe oben) generiert wird.

Vorteile eines cloudbasierten Schlüssels:

- Keine Serverinfrastruktur-Anforderungen auf Kundenseite
- Vereinfachte Freigabe von Daten für Partner und Benutzer anderer Organisationen

Möglichkeiten der Verschlüsselung für Anwender

Auch Anwender können Dateien mit sensiblen Daten verschlüsseln. Unter anderem ist es möglich

- Office-Dateien (Word, Excel, Power Point) zu verschlüsseln,
- in Office-Dateien den Zugriff für bestimmte Personen einzuschränken.
- in OneDrive und SharePoint die Zugriffe zu verwalten und
- private Kanäle in Teams zu erstellen.

Hier liegt die Verantwortung bei der jeweiligen Organisation, Mitarbeitende entsprechend zu sensibilisieren und zu schulen.

Third-Party-Gateways

Neben den von Microsoft angebotenen Verschlüsselungsverfahren existieren eine Reihe von Anbietern am Markt, die eine von Microsoft losgelöste Verschlüsselung anbieten und sich in M365 integrieren lassen. Sogenannte Third-Party-Gateways stellen sicher, dass sensible Informationen sicher verschlüsselt werden, bevor sie an Microsoft übertragen werden.

Die Stärke der autarken Datenverschlüsselung kann jedoch auch zu Nachteilen führen. Z. B. stellt die Volltextsuche in verschlüsselten Daten eine technische Herausforderung dar. Daher eignet sich die Nutzung von Third-Party-Gateways hauptsächlich bei extrem schutzbedürftigen Daten oder wenn regulatorische Vorgaben einen Einsatz von Cloud-Lösungen ohne Third-Party-Gateway unmöglich erscheinen lassen.

Ist die Nutzung von Microsoft Teams bedenkenlos möglich? Auf welche meiner Daten hat Microsoft Zugriff?

Obwohl sich viele datenschutzfreundliche Optionen einstellen lassen, bleibt eine rechtliche Lücke bestehen, da personenbezogene Daten (z. B. Telemetriedaten) übermittelt werden. Die Verwendung von (Video-)Besprechungen bedarf in jedem Fall eines bereits vorhandenen oder zu schaffenden Erlaubnistatbestands.

Die Antwort auf die Frage, ob Microsoft Teams bedenkenlos eingesetzt werden kann, wird wohl “es kommt darauf an” lauten müssen (insbesondere durch die zwingende Übermittlung von Daten der „wesentlichen Dienste“ – u. a. Telemetriedaten). Für die Verarbeitung von personenbezogenen Daten (und auch deren Übermittlung) bedarf es einer Rechtsgrundlage, z. B. im Rahmen des Vertragsverhältnisses, des Beschäftigungsverhältnisses oder mittels einer Einwilligung.

Ist eine gesonderte Rechtsgrundlage für (Video-)Besprechungen in Microsoft Teams erforderlich? Müssen Teilnehmende eine Einwilligung erteilen?[22]

Zunächst einmal bedarf jede Verarbeitung von personenbezogenen Daten einer Rechtsgrundlage. Wenn zudem nicht ausgeschlossen werden kann, dass Daten in ein Drittland übermittelt werden, braucht es auch für diesen Verarbeitungsschritt einer Legitimation. Sofern durch Verwendung von Standarddatenschutzklauseln keine „geeigneten Garantien" geschaffen werden können[23], kann eine Datenübermittlung ungeachtet der dargestellten Zusatzmaßnahmen nur aufrechterhalten werden, wenn ein Ausnahmetatbestand des Art. 49 DSGVO greift.[24]

Für die Kommunikation mit Mitarbeitenden wäre zunächst daran zu denken, die Verarbeitung als erforderlich für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses[25] anzusehen. Sofern man dies anders sehen möchte, bleibt immer noch der Weg, eine Rechtmäßigkeit der Verarbeitung über den Abschluss einer Dienst- oder Betriebsvereinbarung zu erwirken. Betriebsvereinbarungen und andere Kollektivvereinbarungen können nämlich ebenfalls einen Erlaubnistatbestand darstellen.[26] Allerdings fehlt zumindest in der aktuellen Fassung des KDG ein solch klarstellender Zusatz, dass auch ein Tarifvertrag/eine Kollektivvereinbarung als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten herangezogen werden kann.[27]

Die Überlegungen verfangen jedoch nicht bei der Verarbeitung von personenbezogenen Daten außerhalb des Beschäftigungsverhältnisses oder bei der Verarbeitung von Daten Dritter (etwa Kunden oder Lieferanten). In diesem Fall könnte ein berechtigtes Interesse des Verantwortlichen[28] die Rechtsgrundlage für die Datenverarbeitung darstellen. Jedoch ist mit diesem Erlaubnistatbestand eine gewisse Rechtsunsicherheit verbunden, da nicht zwingend davon ausgegangen werden kann, dass die Interessen des Verantwortlichen gegenüber denen der Betroffenen überwiegen. Sind etwa Daten zwingend für die Funktionalität eines Dienstes erforderlich, wie beispielsweise Authentifizierungs- oder Lizenzierungsdaten, können diese bereits auf die Erfüllung eines bestehenden Vertragsverhältnisses gestützt werden.

Für die Verarbeitung von Kunden- oder Lieferantendaten wird man als Rechtsgrundlage wohl auf die Verarbeitung im Rahmen von Vertragsbeziehungen[29] abstellen dürfen.

Natürlich kann man die Verarbeitung von personenbezogenen Daten alternativ auch über die Einholung einer Einwilligung des Betroffenen legitimieren. Allerdings muss sich der Verantwortliche darüber im Klaren sein, dass ein Betroffener seine Einwilligung jederzeit widerrufen kann. Zudem steht man vor der Aufgabe, die Einwilligung korrekt einzuholen. Der zusätzliche Preis ist ein erheblicher Organisations- und Dokumentationsaufwand, um die Einwilligung sowie die aus dieser resultierenden Möglichkeit eines Widerrufs zu verwalten.

Überlegungen, wie eine Übermittlung von personenbezogenen Daten in Drittstaaten gestaltet werden muss, wird ab Seite 35 thematisiert. Zusätzlich sind Maßnahmen zur Datenminimierung zu ergreifen. So sollten beispielsweise geteilte Dokumente nicht unendlich lange archiviert werden, sensible Informationen nur verschlüsselt abgelegt und geteilt werden, Aufzeichnungen nur mit der Einwilligung der betroffenen Personen angefertigt werden, usw.

---

[22] Siehe zur grundsätzlichen Thematik: „Orientierungshilfe Videokonferenzsysteme“ der DSK unter https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf, zuletzt abgerufen am 30.01.2021
[23] Siehe Frage 8 mit Details zum Schrems II-Urteil
[24] Ausführliche Darstellung siehe Johnson/Brechtel: Schrems. Der Tragödie zweiter Teil, ITRB 2020, S. 285 (S. 288 f.)
[25] i. S. v. § 26 BDSG (im Bereich des Kirchendatenschutzes: § 53 KDG bzw. § 49 DSG-EKD)
[26] Siehe Art. 88 DSGVO bzw. § 49 Abs. 1 DSG-EKD.
[27] Wenn man solche Kollektivvereinbarungen als Vertrag werten möchte, ist § 6 Abs. 1 lit. c KDG die anwendbare Rechtsgrundlage.
[28] nach Art. 6 Abs. 1 lit. f) DSGVO (resp. § 6 Abs. 1 lit. b KDG bzw. § 6 Abs. 8 DSG-EKD)
[29] Art. 6 Abs. 1 lit. b) DSGVO, § 6 Abs. 1. lit. c) KDG, § 6 Nr. 5 DSG-EKD

Kann ich Microsoft daran hindern, meine Daten einzusehen?

Grundsätzlich werden drei Arten von Daten an Microsoft übermittelt: „Diagnosedaten“, „verbundene Dienste”-Daten und „wesentliche Dienste”-Daten. Die Übermittlung der beiden erstgenannten Daten lässt sich vollständig unterbinden, “wesentlichen Dienste” -Daten werden jedoch zwingend übermittelt.

Die Daten, die an Microsoft über Microsoft 365-Apps gesendet werden, können in drei Kategorien unterteilt werden (Diagnosedaten, „Verbundene Erfahrungen“-Daten, „wesentliche Dienste“-Daten):

Anfallende Daten bei der Nutzung von M365 und ihre Übertragung in die USA		
Datentyp	**Beschreibung**	**Übertragung in die USA**
Diagnosedaten	Technische Informationen, die Microsoft helfen, Office sicher und auf dem neuesten Stand zu halten, Probleme zu erkennen und zu beheben.	Ja (Deaktivierung möglich)
„Verbundene Erfahrungen“-Daten	Dienste, die Office-Inhalte nutzen, um Bearbeitungsvorschläge und ähnliche Funktionen bereitzustellen. Dienste, die das Suchen und Herunterladen von Onlineinhalten ermöglichen, bspw. Office-Vorlagen.	Ja (Deaktivierung möglich)
„wesentliche Dienste“-Daten	Technische Informationen, die für die Funktionalität von M365 erforderlich sind, bspw. Authentifizierung, Microsoft AutoUpdate oder Telemetrie.	Ja
Data at Rest	Inhalte des Anwenders im Ruhezustand, bspw. Dateien in einer SharePoint-Bibliothek oder E-Mail-Nachrichten und Anlagen in Ordnern von E-Mail-Postfächern.	Nein, Verarbeitung in der jeweils gewählten Zone*.
Data in Transit	Inhalte des Anwenders in Übermittlung, bspw. E-Mail-Nachrichten, die gerade zugestellt werden, oder Unterhaltungen, die in einer Onlinebesprechung stattfinden.	Nein, Verarbeitung in der jeweils gewählten Zone*.

**) Der Clarifying Lawful Overseas Use of Data-Act („CLOUD-Act“)[30] sieht vor, dass US-amerikanische Geheimdienste und Strafverfolgungsbehörden auf Daten von Kunden US-amerikanischer Firmen zugreifen dürfen – auch wenn diese Daten auf den Servern der europäischen Töchter von US-Unternehmen liegen. Microsoft geht jedoch grundsätzlich gegen jede dieser Behördenanfragen juristisch vor, häufig mit Erfolg.[31]*

[30] Siehe hierzu auch Frage 8
[31] Vgl. Microsoft Law Enforcement Requests Report, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report, letzter Abruf am 14.07.2022.

Die nachfolgende Darstellung der drei Kategorien entspricht der Darstellung von Microsoft: [32]

Diagnosedaten (Diagnosedaten, die von Microsoft 365 Apps for Enterprise an Microsoft gesendet werden)

Diagnosedaten werden dazu verwendet, Office sicher und auf den neuesten Stand zu halten, Probleme zu erkennen, zu diagnostizieren und zu beheben sowie Produktverbesserungen vorzunehmen. In diesen Daten sind weder Namen oder E-Mail-Adresse eines Benutzers noch Inhalte von Dateien des Benutzers oder Informationen über Anwendungen enthalten, die nichts mit Office zu tun haben.

Diese Diagnosedaten werden gesammelt und an Microsoft gesendet, um die Verwendung von Office-Clientsoftware auf dem Gerät des Benutzers in Ihrer Organisation zu überprüfen.

Es gibt drei Ebenen von Diagnosedaten für die Microsoft 365 Apps for Enterprise-Clientsoftware, aus denen Sie wählen können:

> **Erforderlich** - Die Mindestdaten, die erforderlich sind, um sicherzustellen, dass Office auf dem Gerät, auf dem es installiert ist, auf dem neuesten Stand ist sowie sicher und erwartungsgemäß funktioniert.
>
> **Optional** - Zusätzliche Daten, die uns helfen, Produktverbesserungen vorzunehmen und erweiterte Informationen liefern, die uns helfen, Probleme zu erkennen, zu diagnostizieren und zu beheben.
>
> **Weder noch** - Es werden keine Diagnosedaten über die auf dem Gerät des Benutzers ausgeführte Office-Clientsoftware gesammelt und an Microsoft gesendet. Diese Option schränkt jedoch unsere Möglichkeiten zur Erkennung, Diagnose und Behebung von Problemen erheblich ein, auf die Ihre Benutzer bei der Verwendung von Office stoßen könnten.

Erforderliche Diagnosedaten können z. B. Informationen über die auf dem Gerät installierte Version von Office sein oder Informationen beinhalten, die darauf hindeuten, dass Office-Anwendungen beim Versuch, Dokumente zu öffnen, abstürzen. Optionale Diagnosedaten können Informationen, über die zum Speichern eines Dokuments erforderliche Zeit beinhalten, was auf ein spezielles Problem beim Speichern auf Ihrem Gerät hinweisen könnte.

Wenn Sie sich dafür entscheiden, uns optionale Diagnosedaten zu senden, werden auch die erforderlichen Diagnosedaten mitgeliefert.

Als Administrator für Ihr Unternehmen können Sie anhand einer Richtlinieneinstellung auswählen, welche Ebene von Diagnosedaten an uns gesendet wird. Optionale Diagnosedaten werden an Microsoft gesendet, es sei denn, Sie ändern die Einstellung. Die Bereitstellung optionaler Diagnosedaten ermöglicht es dem Office-Entwicklerteam von Microsoft, Probleme zu erkennen, zu diagnostizieren und zu beheben, um die Auswirkungen auf Ihr Unternehmen zu minimieren.

Wenn Benutzer mit den organisatorischen Anmeldeinformationen (auch als Geschäfts-, Schul- oder Uni-Konto bezeichnet) bei Office angemeldet sind, können sie die Diagnosedatenebene für ihre Geräte nicht ändern.

In diesen Diagnosedaten sind weder Namen oder E-Mail-Adressen von Benutzern noch Inhalte von Dateien der Benutzer enthalten. Unser System erstellt eine eindeutige ID und verknüpft diese mit den Diagnosedaten des Benutzers. Wenn wir Diagnosedaten erhalten, die zeigen, dass eine unserer Apps 100-mal abgestürzt ist, können wir mit dieser eindeutigen ID feststellen, ob es ein einzelner Benutzer war, der 100 Mal abgestürzt ist, oder ob es 100 verschiedene Benutzer waren, die jeweils einmal abgestürzt sind.

[32] Vgl. hierzu und im Folgenden https://docs.microsoft.com/de-de/deployoffice/privacy/overview-privacy-controls, zuletzt abgerufen am 14.07.2022

Microsoft verwendet diese eindeutige ID nach eigenen Angaben nicht, um einen bestimmten Benutzer zu identifizieren, es handelt sich aber um Daten mit einem Personenbezug.

Verbundene Erfahrungen-Daten (Verbundene Erfahrungen für Microsoft 365 Apps for Enterprise)

Microsoft 365 Apps for Enterprise besteht aus Clientsoftware-Anwendungen und verbundenen Erfahrungen, die es Ihnen ermöglichen, effektiver zu erstellen, zu kommunizieren und zusammenzuarbeiten. Die Zusammenarbeit mit anderen an einem auf OneDrive for Business gespeicherten Dokument oder die Übersetzung des Inhalts eines Word-Dokuments in eine andere Sprache sind Beispiele für verbundene Erfahrungen.

Wir verstehen, dass Sie vielleicht wählen möchten, welche Arten von verbundenen Erfahrungen Ihren Benutzern bei der Arbeit in Office-Anwendungen zur Verfügung stehen. Als Administrator für Ihre Organisation verfügen Sie über Richtlinieneinstellungen, mit denen Sie auswählen können, ob Sie Ihren Benutzern die folgenden Arten von verbundenen Erfahrungen zur Verfügung stellen möchten:

> **Dienste, die Ihre Inhalte analysieren** - Dienste, die Ihre Office-Inhalte nutzen, um Ihnen Designempfehlungen, Bearbeitungsvorschläge, Datenerkenntnisse und ähnliche Funktionen bereitzustellen. Beispiel: PowerPoint-Designer oder Übersetzer.
>
> **Dienste die Onlineinhalte herunterladen** - Dienste, die das Suchen und Herunterladen von Onlineinhalten, einschließlich Vorlagen, Bildern, 3D-Modellen, Videos und Referenzmaterialien, ermöglichen, um Ihre Dokumente zu verbessern. Z. B. Office-Vorlagen oder PowerPoint-Schnellstarter.

Beispielsweise können Sie Ihren Benutzern verbundene Erfahrungen zur Verfügung stellen, die Onlineinhalte herunterladen, nicht aber verbundene Erfahrungen, die Inhalte analysieren. Wenn Sie diese Richtlinieneinstellungen nicht konfigurieren, stehen Ihren Benutzern alle diese verbundenen Erfahrungen zur Verfügung.

Darüber hinaus gibt es eine Richtlinieneinstellung, die es Ihnen ermöglicht, alle diese verbundenen Erfahrungen zu deaktivieren, und die auch andere verbundene Erfahrungen deaktiviert, wie z.B. die gemeinsame Dokumentenerstellung und die Datenspeicherung online. Aber selbst, wenn Sie diese Richtlinieneinstellung verwenden, um alle diese verbundenen Erfahrungen zu deaktivieren, bleiben bestimmte Office-Funktionen verfügbar, wie z. B. die Synchronisierung Ihres Postfachs in Outlook, die Verwendung von Teams oder Skype for Business, sowie die im Folgenden beschriebenen wesentlichen Dienste.

Wenn Sie entscheiden, Ihren Benutzern bestimmte Arten von verbundenen Erfahrungen nicht zur Verfügung zu stellen, wird entweder der Menüband- oder der Menübefehl für diese verbundenen Erfahrungen abgeblendet, oder die Benutzer erhalten eine Fehlermeldung, wenn sie versuchen, diese verbundenen Erfahrungen zu verwenden.

Wenn die Benutzer mit den organisatorischen Anmeldeinformationen (auch als Geschäfts-, Schul- oder Uni-Konto bezeichnet) bei Office angemeldet sind, können sie nicht auswählen, ob sie diese verbundenen Erfahrungen aktivieren oder deaktivieren möchten.

Zusätzlich zu den oben genannten verbundenen Erfahrungen, die in Microsoft 365 Apps for Enterprise enthalten sind, gibt es zusätzliche optionale verbundene Erfahrungen, die Sie auswählen können, um Ihren Benutzern den Zugriff über ihr Geschäftskonto zu ermöglichen. Beispielsweise die LinkedIn-Features des Lebenslauf-Assistenten in Word oder die 3D-Karten-Funktion in Excel, die Bing verwendet.

Dies sind zusätzliche optionale verbundene Erfahrungen, die nicht durch den kommerziellen Lizenzvertrag Ihrer Organisation mit Microsoft abgedeckt sind, sondern durch separate Bedingungen geregelt werden. Optionale verbundene Erfahrungen, die Microsoft Ihren Benutzern direkt anbietet, werden durch den Microsoft-Servicevertrag anstelle der Online Services-Nutzungsbedingungen geregelt.

Da diese optionalen verbundenen Erfahrungen durch separate Geschäftsbedingungen geregelt sind, verwalten Sie sie getrennt von den oben genannten verbundenen Erfahrungen. Als Administrator für Ihre Organisation können Sie anhand einer Richtlinieneinstellung entscheiden, ob Sie Ihren Benutzern diese optionalen verbundenen Erfahrungen als Gruppe zur Verfügung stellen möchten. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, stehen Ihren Benutzern diese optionalen verbundenen Erfahrungen zur Verfügung.

Auch wenn Sie Ihren Benutzern diese optionalen verbundenen Erfahrungen zur Verfügung stellen, haben Ihre Benutzer die Möglichkeit, diese über das Dialogfeld Datenschutzeinstellungen als Gruppe zu deaktivieren. Ihre Benutzer haben diese Wahl nur, wenn sie mit ihren organisatorischen Anmeldeinformationen (auch als Geschäfts-, Schul- oder Uni-Konto bezeichnet) und nicht mit einer persönlichen E-Mail-Adresse bei Office angemeldet sind.

Wesentliche Dienste-Daten

Es gibt auch eine Gruppe von Diensten, die für die Funktionsweise von Microsoft 365 Apps for Enterprise wesentlich sind und nicht deaktiviert werden können. Beispielsweise der Lizenzierungsdienst, der bestätigt, dass Sie über eine ordnungsgemäße Lizenz zur Verwendung von Microsoft 365 Apps for Enterprise verfügen. Erforderlicher Dienstdaten zu diesen Diensten werden erfasst und an Microsoft gesendet, unabhängig von anderen Richtlinieneinstellungen, die Sie konfiguriert haben. Hierzu zählen folgende Dienste:[33]

- Authentifizierung,
- Klick-und-Los,
- Enhanced Configuration Service (ECS),
- Lizenzierung,
- Microsoft AutoUpdate (MAU),
- Synchronisierung durch OneNote,
- Dienste-Konfiguration,
- Telemetrie[34]

[33] Siehe https://docs.microsoft.com/de-de/deployoffice/privacy/essential-services, zuletzt abgerufen am 31.03.2022
[34] Als Telemetriedaten bezeichnet Microsoft diejenigen Daten, die z. B. die Lasten in Rechenzentren oder den Verbrauch der Bandbreite zwischen den Rechenzentren überwachen. Laut eigener Aussage haben diese keinen Personenbezug, sondern dienen lediglich zur Optimierung des Angebots.

Meinung von Microsoft und Aufsichtsbehörden

Microsoft ist der Meinung, dass die bestehenden Standarddatenschutzklauseln, inkl. der eingesetzten Schutzmechanismen von Microsoft, als Instrument für die Übermittlung von personenbezogenen Daten an Drittstaaten (auch in die USA) dienlich sind und weiterhin eine rechtlich legitime Basis darstellen.[35]

Der LfDI Baden-Württemberg hält eine Übermittlung (in die USA) auf Grundlage von Standarddatenschutzklauseln zwar für denkbar, sieht die Anforderungen, die der EuGH an ein wirksames Schutzniveau gestellt hat, jedoch nur in seltenen Fällen erfüllt[36]*:*

Der Verantwortliche muss hier zusätzliche Garantien bieten, die einen Zugriff durch die US-amerikanischen Geheimdienste effektiv verhindern und so die Rechte der betroffenen Personen schützen; dies wäre etwa in folgenden Fällen denkbar:

- *Verschlüsselung, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann*[37]*,*
- *Anonymisierung aller personenbezogenen Daten*

Im Lichte der Diskussion um die Datenschutzkonformität und den Einsatz von Microsoft 365 und Microsoft Teams, z. B. im Bildungssektor, hat Microsoft am 11. August 2022 weitere Informationen zur Haltung des Unternehmens und zum Umgang mit personenbezogenen Daten veröffentlicht. Darin werden einige Vorwürfe und Aussagen aus Sicht von Microsoft kommentiert bzw. korrigiert.[38]

[35] Siehe https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-eu-model-clauses?view=o365-worldwide, zuletzt abgerufen am 14.07.202
[36] Siehe https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/Orientierungshilfe-Was-jetzt-in-Sachen-internationaler-Datentransfer.pdf, zuletzt abgerufen am 14.07.2022
[37] Ob letztendlich Verschlüsselungen existieren, die von „US-Diensten" nicht gebrochen werden können, ist nicht zweifelsfrei nachweisbar
[38] Siehe https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/08/Microsoft-Statement_Datenschutzkonformitaet-von-Microsoft-365-und-Microsoft-Teams.pdf, zuletzt abgerufen am 12.09.2022

III. Besonderheiten im Bereich Kirche & Wohlfahrt

In Kirche und Wohlfahrt ist der Schwerpunkt der Verarbeitung personenbezogener Daten im Vergleich zu Unternehmen der freien Wirtschaft verlagert. Es liegt in der Natur der Sache, dass hier regelmäßig Sozial- und Gesundheitsdaten verarbeitet werden und Berufsgeheimnisse einschlägig sind. Hinzu kommt bei kirchlichen Trägern, dass sie unter kirchliches Datenschutzrecht fallen, aus dem sich eigene Bedingungen für die Nutzung von M365 ergeben können.

Welche Besonderheiten sind für katholische Organisationen zu beachten, die unter KDG oder KDR-OG fallen?

Der katholische Datenschutz folgt weitgehend der weltlichen Gesetzgebung von DSGVO und BDSG. Jedoch muss in AV-Verträgen die entsprechende Rechtswahl berücksichtigt werden. Für die Drittlandübermittlung können de facto die Bedingungen aus dem weltlichen Recht vorausgesetzt werden, während de jure andere Bestimmungen vorliegen. Was die Informationssicherheit angeht, sind die Präzisierungen der technischen und organisatorischen Maßnahmen in der KDG-DVO zu beachten.

Auftragsverarbeitung

Die Regelungen zur Auftragsverarbeitung im KDG folgen weitestgehend der DSGVO, sodass inhaltlich keine Schwierigkeiten entstehen dürften.[39] Ein Verantwortlicher, der unter das KDG fällt, muss dies entweder im AV-Vertrag durch einen Passus zur Rechtswahl festhalten oder eine entsprechende Nebenabrede mit Microsoft treffen. Microsoft muss sich dabei nicht dem KDG oder den katholischen Datenschutz-Aufsichtsbehörden unterwerfen. Es empfiehlt sich jedoch, zumindest die Bereitschaft zur Zusammenarbeit mit den kirchlichen Datenschutzaufsichten bestätigen zu lassen..[40]

Einer der Unterschiede zum weltlichen Recht besteht darin, dass das KDG die „Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen“ durch Dienstleister explizit als Auftragsverarbeitung hervorhebt, wenn dabei ein Zugriff auf personenbezogene Daten nicht per se ausgeschlossen werden kann.[41]

Präzisiert werden die Bedingungen hierfür in der „Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz“ (KDG-DVO).[42] Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands bietet vor diesem Hintergrund eine eigene Arbeits- und Formulierungshilfe "Vertrag zur Fernwartung zwischen kirchlichem Auftraggeber und nichtkirchlichem Auftragnehmer" an.

[39] Die Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) stimmt hiermit soweit überein, dass alle Aussagen zum KDG auch für die entsprechenden Passus in der KDR-OG Geltung haben.
[40] Vgl. § 32 KDG. Dass es wichtig ist, die Rechtswahl des katholischen Datenschutzrechts vertraglich zu fixieren, zeigt ein arbeitsrechtliches Urteil, in dem das LAG Köln sein Urteil mit dem Verstoß einer Pfarrangestellten gegen § 26 BDSG begründet (Urteil vom 02.11.2021, Az. 4 Sa 290/21, Rn. 46), obwohl ihre Tätigkeit eigentlich unter das KDG fällt.
[41] § 29 Abs. 12 KDG.
[42] § 21 KDG-DVO i.V.m. § 15 Abs. 5 KDG-DVO. Die Durchführungsverordnung zur Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG-DVO) stimmt hiermit weitestgehend überein, so dass alle Aussagen zur KDG-DVO auch für die entsprechenden Passus in der KDR-OG-DVO Geltung haben.

Drittlandübermittlung

Das Problem der Datenübermittlung an Empfänger außerhalb der EU ist im katholischen Datenschutz gegenüber der DSGVO deutlich kürzer gefasst, sodass nicht alle Wege der Legitimation beschritten werden können.[43]

Standarddatenschutzklauseln kennt das KDG nicht explizit[44]. Hier wurde jedoch eine Bestimmung aus dem BDSG übernommen, der zufolge „in einem rechtsverbindlichen Instrument geeignete Garantien" festgelegt werden dürfen,[45] sodass nach denselben Maßgaben wie im weltlichen Datenschutz verfahren werden kann. Dabei wäre nach strenger Auslegung der Einsatz von Standarddatenschutzklauseln im Rahmen von Auftragsverarbeitung für katholische Einrichtungen gar nicht zulässig, da sich der Wortlaut des § 29 Abs. 11 KDG ausschließlich auf § 40 Abs. 1 KDG bezieht und die rechtsverbindlichen Instrumente erst durch den folgenden Absatz ermöglicht werden. Hierbei handelt es sich wohl um einen redaktionellen Fehler im Gesetz, der möglicherweise 2023 korrigiert werden wird.

Das katholische Datenschutzzentrum in Dortmund hat auf Anfrage zu verstehen gegeben, dass Standarddatenschutzklauseln de facto als geeignete Garantien herangezogen werden können.[46] Es gelten jedoch auch hier die Einschränkungen des EuGH-Urteils vom Sommer 2020 – weitere Maßnahmen und Garantien müssen ergänzt werden (siehe hierzu „Werden beim Einsatz von M365 personenbezogene Daten in Länder außerhalb Europas wie z. B. die USA übermittelt?" Ab Seite 35).

In § 40 Abs. 2 lit. B KDG ist auch die leicht veränderte Bestimmung aus dem BDSG eingeflossen, dass der Verantwortliche personenbezogene Daten in Drittländer übermitteln darf, wenn er „nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, davon ausgehen kann, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen."[47] Damit wird die Bewertungshoheit aus den Händen der Europäischen Kommission in die des Verantwortlichen gelegt, was im Zweifelsfall kaum standhalten würde. Von einer Drittlandübermittlung auf Basis dieser Selbstzertifizierung ist abzuraten, da sie nicht die erforderliche Rechtssicherheit aufweist.

Technische und organisatorische Maßnahmen

Das KDG folgt den Bestimmungen der DSGVO zur Sicherheit der Verarbeitung weitestgehend. Ergänzend wurde jedoch im November 2018 die KDG-DVO erlassen, in der die technischen und organisatorischen Maßnahmen (TOM) konkretisiert werden, die der Verantwortliche zu treffen hat. In technischer Hinsicht entstehen hieraus keine besonderen Probleme für die Nutzung von M365, jedoch muss organisatorisch einiges beachtet werden.

So muss der Verantwortliche ein Datenschutzkonzept erstellen.[48] Hierfür definiert die KDG-DVO vier Datenschutzklassen (I, II und III sowie „Daten, die dem Beicht- oder Seelsorgegeheimnis unterliegen"), in

[43] Art. 44-50 DSGVO gegenüber §§ 39-41 KDG. Der nunmehr hinfällige EU-US Privacy Shield war im Sinne eines Angemessenheitsbeschlusses der EU gem. § 40 Abs. 1 KDG anwendbar.
[44] Vgl. Art. 46 Abs. 2 lit. c & d DSGVO
[45] § 40 Abs. 2 lit. a KDG.
[46] Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche vertritt folgende Auffassung: *„In § 29 Abs. 11 KDG wird zwar explizit nur auf § 40 Abs. 1 KDG verwiesen, doch schließt der Wortlaut der gesamten Vorschrift einen Verweis auf § 40 Abs. 2 ebenso mit ein. § 29 Abs. 11 erlaubt nämlich die Feststellung durch die zuständige oder eine andere Datenschutzaufsicht, dass im Drittstaat ein angemessenes Datenschutzniveau besteht. Nichts anderes bedeutet der Inhalt des § 40 Abs. 2 KDG wenn auch mit der Maßgabe, dass die Feststellung durch eine Datenschutzaufsicht getroffen werden muss und nicht durch den Verantwortlichen selbst."* Zitiert nach Andreas Hellmann, Übermittlung und Verarbeitung personenbezogener Daten außerhalb der EU, https://www.althammer-kill.de/news-detail/uebermittlung-und-verarbeitung-personenbezogener-daten-ausserhalb-der-eu, Abruf am 27.10.2020.
[47] § 40 Abs. 2 lit. b KDG.
[48] § 15 Abs. 4 KDG-DVO. Das Erzbistum München und Freising stellt eine Mustervorlage „Datenschutzkonzept" zur Verfügung: https://www.erzbistum-muenchen.de/media/old/media28712226.DOCX.

welche auf Basis einer systematischen Risikoanalyse sämtliche Daten eingeordnet werden müssen. weiterhin werden entsprechende Datenschutzniveaus definiert, die es einzuhalten gilt.[49]

Eine automatisierte Lösung, nach der sich die Datenschutzklassen in M365 implementieren und mit entsprechenden Regeln versehen ließen, dürfte nur mit erheblichem Aufwand und zudem nicht für alle Lizenzmodelle umsetzbar sein. Organisationen sind hierdurch jedoch in der Pflicht, selbst entsprechende Konzepte zu erstellen, die organisatorische Vorgaben für Anwender bieten, um die Anforderungen der KDG-DVO zu erfüllen.

Zusatzvereinbarungen

Auch für Verantwortliche unter katholischem Datenschutzrecht besteht das Erfordernis zum Abschluss von Zusatzvereinbarungen, um die Wahrung von Berufsgeheimnissen nach weltlichem Recht zu gewährleisten (hierzu detaillierter „Welche spezialgesetzlichen Bestimmungen gilt es zu beachten?“ ab Seite 26).

Positionen der katholischen Datenschutzaufsichten

Das KDSZ Dortmund hat sich zuletzt im Jahresbericht 2019 zur „Cloud-Nutzung durch kirchliche Stellen“ positioniert,[50] also noch vor dem Schrems-II-Urteil. Im Wesentlichen wird hier auf mangelnde Transparenz bei der Übermittlung von Daten in Drittländer verwiesen sowie auf den US-amerikanischen CLOUD-Act. Auf eine klare Richtungsempfehlung wird offenbar verzichtet und letztlich im Sinne dieses Whitepapers auf die Verantwortung der jeweiligen Organisation abgestellt:

> *„Bei der Bewertung der Risiken müssen alle Einrichtungen unabhängig von dem ausgewählten Anbieter die oben erwähnten Grundrisiken mit bewerten und wenn der Einsatz der Produkte für die Einrichtung unverzichtbar ist Strategien entwickeln, wie trotzdem ein datenschutzkonformer Betrieb möglich ist.“*

Der Datenschutzbeauftragte der bayerischen (Erz-)Diözesen urteilt demgegenüber vor dem Hintergrund von Schrems-II in Bezug auf M365:[51]

> *„Wie die öffentlichen Dienststellen sollten kirchliche keine Cloud-Anwendungen für die Übertragung personenbezogener Daten nutzen, bei denen der physikalische Datenspeicher sich außerhalb des Gebiets der EU befindet.“*

Da das Regionen-Modell von Microsoft ohne Rechenzentren außerhalb der EU auskommt (hierzu mehr ab Seite 35), sollte hierin in Bezug auf physikalische Datenspeicher eigentlich kein Problem bestehen. Zentraler Kritikpunkt ist jedoch die Möglichkeit des Zugriffs durch US-Behörden auf Grundlage des CLOUD-Acts. In einer anderen Stellungnahme heißt es zu Cloud-Diensten von US-Anbietern daher:[52]

> *„Es gibt bisher keinen vernünftigen Grund zur Aufhebung des Verbotes“.*

[49] §§ 9-14, 25 KDG-DVO.
[50] Katholisches Datenschutzzentrum Dortmund, Jahresbericht 2019, https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2021/07/Jahresbericht-2019.pdf https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2020/09/Jahresbericht-2019.pdf, Abruf am 07.03.2022. Vgl. auch Katholisches Datenschutzzentrum Frankfurt/M., Datenschutzrechtliche Bewertung eines Einsatzes von Office 365 auf der Plattform der Microsoft Cloud, https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/MS-Cloud-2019-KDSZ-FFM.pdf, Abruf am 07.03.2022.
[51] Erzdiözese München und Freising, Datenschutzaufsicht, Cloud- und Meeting-Programme, https://www.erzbistum-muenchen.de/ordinariat/datenschutzstelle/webbasierte-anwendungen/99282, Abruf am 07.03.2022.
[52] Erzdiözese München und Freising, Datenschutzaufsicht, Wie soll die Datenschutzaufsicht der Katholischen Kirche in Bayern mit dem Urteil des Europäischen Gerichtshofs (Schrems II) vom 16. Juli 2020 umgehen?, https://www.erzbistum-muenchen.de/cms-media/media-51947220.pdf, Abruf am 07.03.2022.

Welche Besonderheiten sind für evangelische Organisationen zu beachten, die unter das DSG-EKD fallen?

Organisationen, die unter das DSG-EKD fallen, benötigen zum Vertrag zur Auftragsverarbeitung (DPA) noch eine Zusatzvereinbarung („Unterwerfung unter die kirchliche Datenschutzaufsicht"). Des Weiteren sind die von der Europäischen Kommission beschlossenen Standarddatenschutzklauseln für die Übermittlung von personenbezogenen Daten heranzuziehen und an den Einzelfall anzupassen.

Auch für das DSG-EKD gilt, dass es ähnlich wie im weltlichen Bereich gehandhabt wird. Jedoch ist der Vertrag zur Auftragsverarbeitung mit einer Zusatzvereinbarung zu versehen, in der sich der Auftragsverarbeiter der kirchlichen Datenschutzaufsicht unterwirft.[53] Des Weiteren müssen Standarddatenschutzklauseln und zusätzliche Maßnahmen/Garantien vereinbart werden.

Auftragsverarbeitung

Auch im Bereich der EKD sind mit Auftragsverarbeitern Verträge zur Auftragsverarbeitung zu schließen. Sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden, ist die kirchliche Stelle verpflichtet sicherzustellen, dass der Auftragsverarbeiter die DSG-EKD oder gleichwertige Bestimmungen beachtet (z. B. die DSGVO).

Grundsätzlich ist es also möglich, einen AV-Vertrag auf Basis der DSGVO zu schließen. Allerdings muss sich der Auftragsverarbeiter der kirchlichen Datenschutzaufsicht unterwerfen.[54] Da dieser Passus in dem Standard-DPA von Microsoft nicht enthalten ist, müssen Organisationen eine Zusatzvereinbarung mit Microsoft abschließen. Hierzu äußerte sich der Beauftragte für den Datenschutz der EKD (BfD EKD) im Februar 2020 wie folgt:

> *„Zusätzlich zu diesem Vertrag [zur Auftragsverarbeitung] muss mit Microsoft eine Zusatzvereinbarung geschlossen werden, bei der sich Microsoft der kirchlichen Datenschutzaufsicht unterstellt. [..] Diese Zusatzvereinbarung ist nun von Microsoft in mehreren Fällen unterzeichnet worden, sodass sie auch als Muster für weitere Verhandlungen genutzt werden kann."*[55]

Die Stellungnahme ist weiterhin abrufbar und wurde bislang nicht aktualisiert. Eine entsprechende Vereinbarung bietet Microsoft für Kunden im Enterprise-Umfeld ab 250 Arbeitsplätzen an.

Übermittlung personenbezogener Daten in die USA auf Basis von Standarddatenschutzklauseln

Bei der Verwendung von M365-Diensten werden personenbezogene Daten in die USA übermittelt. Während der AV-Vertrag in Kombination mit der Zusatzvereinbarung die Verarbeitung beim Dienstleister regelt, bedarf es für die Übermittlung der personenbezogenen Daten einer Rechtsgrundlage. Diesbezüglich existieren im § 10 Abs. 1 und 2 DSG-EKD Rechtsgrundlagen, die eine Übermittlung legitimieren können:

§ 10 Abs. 2 Nr. 1-6 DSG-EKD dürften bei der Nutzung von M365-Diensten nur in seltenen Fällen als Rechtsgrundlage dienen. Anders als im weltlichen Bereich stellt die Einwilligung zur Übermittlung (§ 10 Abs. 2 Nr. 1 DSG-EKD) im kirchlichen Recht keinen Ausnahmetatbestand dar. Jedoch ist die Einwilligung im Kontext des Beschäftigtendatenschutzes nur schwer umzusetzen. Ebenso wird die Widerrufbarkeit bei einer Übermittlung von personenbezogenen Daten von einer Vielzahl von Personen als hoher

[53] Siehe hierzu § 30 Abs. 5 DSG-EKD und in 6. „Welche Besonderheiten sind für Organisationen zu beachten, die unter das DSG-EKD fallen?"
[54] § 30 Abs. 5 S. 3 DSG-EKD.
[55] Vgl. https://datenschutz.ekd.de/2020/02/14/nutzung-von-microsoft-cloud-diensten/, zuletzt abgerufen am 31.03.2022

Unsicherheitsfaktor angesehen. Daher sieht der BfD EKD die Einwilligung nur für einzelne Datenübermittlungen als geeignet an, die eine überschaubare Anzahl von Personen betrifft.[56]

Erfolgsversprechender erscheinen Übermittlungen auf Basis von Standarddatenschutzklauseln. Obwohl diese von der Europäischen Kommission für den Geltungsbereich der DSGVO konzipiert wurden, sind diese auch für kirchliche Stellen, die unter das DSG-EKD fallen, anwendbar. Für Datenübermittlungen in die USA ist der bloße Abschluss von Standarddatenschutzklauseln jedoch nicht ausreichend.

Es müssen weitere vertragliche, technische und organisatorische Maßnahmen ergänzt werden, die ein gleichwertiges Schutzniveau (in Relation zur Verarbeitung in DE bzw. der EU/EWR) gewährleisten. Geeignete Maßnahmen können beispielsweise die Pseudonymisierung oder die Verschlüsselung darstellen. Eine Übermittlung von Klardaten wird hingegen als problematisch eingestuft.

Cloud-Entschließung

BfD EKD hat im April 2019 eine Cloud-Entschließung[57] veröffentlicht, die eine Verwendung von Microsoft-Cloud-Diensten datenschutzkonform möglich erscheinen lässt. Die Voraussetzungen sind:

1. Es wird von Microsoft eine wirksame Zusatzvereinbarung angeboten (siehe oben).
2. Eine Verschlüsselung der Daten ohne Zugang von Microsoft ist möglich. (HYOK = Hold your own Key)[58]
3. Die Übersendung von Telemetriedaten kann durch entsprechende Einstellungen unterbunden werden.

Zu 1.: Eine Zusatzvereinbarung wird von Microsoft angeboten und ist in mehreren Fällen abgeschlossen worden. Diese steht jedoch nicht für alle Lizenzformen/Vertragsvarianten zur Verfügung.

Zu 2.: Prinzipiell existiert eine HYOK-Lösung für viele Microsoft-Dienste. Besonders sensible Daten können so wirkungsvoll vor unbefugten Zugriffen geschützt werden. Allerdings beinhaltet eine HYOK-Lösung auch Nachteile. Werden z. B. E-Mails verschlüsselt und liegt der "Key" auf lokalen Speichermedien, kann es zu Einschränkungen bei der Verarbeitung auf dem Cloud-Server kommen. Im Extremfall müssen beim Durchsuchen alle verschlüsselten E-Mails heruntergeladen werden, damit diese auf der lokalen Infrastruktur durchsucht werden können (nach der Entschlüsselung). Third Party Gateways können eine passende Alternative darstellen.

Zu 3.: Telemetriedaten fallen unter die „wesentlichen Dienste", deren Übermittlung kann daher nicht unterbunden werden.

Position des Beauftragten für den Datenschutz der EKD

In jüngeren Äußerungen hat der BfD EKD darauf hingewiesen, dass nach seiner Auffassung eine Datenschutz-Folgenabschätzung (DSFA) im Sinne des § 34 DSG-EKD bei Einsatz von Microsoft 365 durchzuführen ist. Begründet wird dies damit, dass es sich um eine Verwendung neuer Technologien handelt und bei der Verarbeitung von personenbezogenen Daten ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Die Haltung des BfD EKD zur Durchführungspflicht einer Transfer-Folgenabschätzung (Transfer Impact Assessment – kurz: TIA) ist indes noch nicht bekannt. Es ist jedoch erwartbar, dass sich der BfD EKD der weltlichen Meinung anschließen wird und im Rahmen einer Übermittlung somit eine DSFA und ein TIA durchzuführen sind.

---

[56] Siehe hierzu https://datenschutz.ekd.de/wp-content/uploads/2021/10/GemeinsameStellungnahmeDatenuebermittlungUSA.pdf Seite 7f., zuletzt abgerufen am 31.03.2022
[57] Siehe hierzu und im Folgenden https://datenschutz.ekd.de/wp-content/uploads/2019/04/Entschlie%C3%9Fung_Microsoft.pdf, zuletzt abgerufen am 08.10.2020
[58] Interessanterweise wird nicht gefordert, dass HYOK tatsächlich aktiviert sein muss.

Denn auch von kirchlicher Seite wird ein gleichwertiges Schutzniveau sowie die Anonymisierung bzw. Pseudonymisierung von personenbezogenen Daten verlangt, sodass „ausländische Behörden“ keine Möglichkeit haben, die Daten auf einzelne Personen zurückzuführen. [59]

Welche spezialgesetzlichen Bestimmungen gilt es zu beachten?

In den spezialgesetzlichen Regelungen steckt, sofern für den Arbeit- resp. Dienstgeber einschlägig, jede Menge Regelungsgehalt, mit dem es sich zu beschäftigen gilt. Relevant sind hier u. a. die Schweigepflicht (§ 203 StGB), Krankenhausgesetzgebung und das Telekommunikationsgesetz (TKG). Zwar kann in Hinblick auf das TKG etwa private E-Mail- und Internetnutzung am Arbeitsplatz per se untersagt werden, um den Regelungsbedarf zu minimieren, doch auch diese Entscheidung fordert ein aktives Handeln des Arbeit- bzw. Dienstgebers.

Heilberufe, Psychologen und Mitarbeitende von Beratungsstellen

Für Angehörige eines Heilberufes und den in § 203 Abs. 1 StGB genannten Personenkreis ist die dort gesetzlich verpflichtende Geheimniswahrung von besonderer Bedeutung. Gemäß § 203 StGB wird derjenige, der unbefugt ein fremdes Geheimnis aus dem persönlichen oder geschäftlichen Bereich offenbart, das ihm bspw. als Arzt, Angehöriger eines Heilberufes oder Sozialpädagoge (nachfolgend „Berufsgeheimnisträger“) anvertraut worden ist, mit Freiheits- oder Geldstrafe bestraft. Zu einer Offenbarung muss die entsprechende Befugnis des Betroffenen vorliegen.

Kein Offenbaren liegt nach § 203 Abs. 3 StGB vor, wenn der Berufsgeheimnisträger das Geheimnis einem bei ihm tätigen Gehilfen, etwa Pflegepersonal, zugänglich macht. Für die Auslagerung von IT-Leistungen hilft diese rechtliche Ausnahme allerdings nicht weiter.

Insofern hat der Gesetzgeber darüber hinaus klarstellend geregelt, dass Berufsgeheimnisträger (auch) sonstigen Personen fremde Geheimnisse offenbaren dürfen, sofern sie an der beruflichen oder dienstlichen Tätigkeit mitwirken und die Mitwirkung für die Inanspruchnahme der Tätigkeit erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese Personen sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der Berufsgeheimnisträger mitwirken.

Unter diese mitwirkenden Tätigkeiten fallen Einrichtung, Betrieb, Wartung und Pflege von informationstechnischen Anlagen, Anwendungen und Systemen.[60] Insofern erfolgt die Offenbarung gegenüber einem IT-Dienstleister nicht unbefugt bzw. rechtswidrig, sofern die Tätigkeiten des IT-Dienstleisters weisungsabhängig erbracht werden.

Der Berufsgeheimnisträger muss dafür Sorge tragen, dass sonstige mitwirkende Personen zur Geheimhaltung nach § 203 StGB verpflichtet sind. Im Falle der Erbringung von bspw. Wartungs- und Supportleistungen durch IT-Dienstleister muss insofern ein Vertrag zur Auftragsverarbeitung und zusätzlich eine entsprechende Verschwiegenheitsverpflichtung nach § 203 StGB mit dem IT-Dienstleister geschlossen werden.

Abhängig von Bezugsmodell und Lizenzierung bietet Microsoft neben dem Abschluss der Online Service Terms und des Data Processing Agreement hier die Möglichkeit, die Vereinbarung ID M657 (Verletzung

[59] Siehe https://datenschutz.ekd.de/wp-content/uploads/2021/10/GemeinsameStellungnahmeDatenuebermittlungUSA.pdf Seite 8, zuletzt abgerufen am 31.03.2022

[60] Vgl. dazu auch Seite 23 der Gesetzesbegründung, verfügbar unter https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/ReGE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 06.01.2021

von Privatgeheimnissen) mit Microsoft abzuschließen. Mittels der Vereinbarung wird Microsoft zusätzlich vertraglich darauf verpflichtet, Daten von Berufsgeheimnisträgern streng vertraulich zu behandeln.

Telemedizin (Videosprechstunde)

Erst jüngst hat das OLG Hamburg[61] entschieden, dass das Angebot der Ausstellung einer Arbeitsunfähigkeitsbescheinigung nach Beantwortung eines Online-Fragenkatalogs und dessen Übermittlung an einen Arzt ohne Rückfragen durch diesen nicht den gesetzlichen Voraussetzungen entspricht und unlauter ist. Dabei sind Fernbehandlungen und deren Bewerbung – Stand heute – nicht per se verboten oder unlauter. Sie müssen sich allerdings an die fachlichen und technischen Standards halten. Zwingende Voraussetzung ist zunächst, dass sich Patient und Arzt bereits persönlich aus vorangegangenen Behandlungen bekannt sind. In fachlicher Hinsicht muss eine telemedizinische Beratung zudem unter Einhaltung ärztlicher Sorgfalt vertretbar sein. Dies bedarf im konkreten Arzt-Patienten-Verhältnis einer Einzelfallprüfung durch den behandelnden Arzt bzw. die behandelnde Ärztin.

In technischer Hinsicht dürfen in der telemedizinischen Versorgung nur Videokonferenzdienste von zertifizierten Anbietern eingesetzt werden. Hintergrund dieser Einschränkung sind die Regelungen aus Anlage 31b „Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V“ zum Bundesmantelvertrag-Ärzte (BMV-Ä).[62]

Dort sind u. a. Bestimmungen resp. Anforderungen an die Informationstechniksicherheit und den Datenschutz zur Durchführung von Videosprechstunden in der vertragsärztlichen Versorgung“ festgeschrieben. Diese Anforderungen muss der Videodienstanbieter durch spezielle Zertifizierungen (für Informationstechniksicherheit gemäß der VO (EG) 765/2008 nach ISO/IEC 17065 und für Datenschutz gemäß Artikel 42 DS-GVO von einer nach ISO/IEC 17065 akkreditierten Zertifizierungsstelle) nachweisen, um in der vertragsärztlichen Versorgung als Videodienst genutzt werden zu dürfen, sprich er benötigt eine Bescheinigung nach § 5 Absatz 2 f. Anlage 31b BMV-Ä.

Alle nach Anlage 31b zertifizierten Videodienste können ausnahmslos über einen Browser genutzt werden und müssen Peer-to-Peer (P2P) erfolgen. Microsoft Teams erfüllt diese Voraussetzungen nicht bzw. nur innerhalb des eigenen Netzwerkes und ist daher nicht als Videodienst für den Bereich Telemedizin zertifiziert. Die Nutzung eines nicht zertifizierten Dienstes stellt einen Verstoß des Arztes gegen seine vertragsärztlichen Pflichten dar und kann gemäß den Disziplinarordnungen der Krankenversicherungen entsprechend geahndet werden.

Sozialgesetze

§ 35 SGB I ist die grundlegende Norm des Sozialdatenschutzes und regelt das Sozialgeheimnis. Das Sozialgeheimnis schützt denjenigen, der in der gesetzlichen Sozialversicherung versichert ist, vor unberechtigten staatlichen Eingriffen oder unbefugten Verarbeitungen. Eine Legaldefinition des Sozialdatums ist in § 67 Abs. 2 SGB X enthalten.

Das Sozialgeheimnis gilt zunächst nur für Sozialleistungsträger[63]. Allerdings finden die Vorschriften des SGB auch auf Rechtsträger Anwendung, die im Wege der Auftragsverarbeitung für Sozialleistungsträger Daten verarbeiten. Zudem gilt der datenschutzrechtliche Grundsatz, dass Sozialdaten, die einer nicht in § 35 SGB I genannten Person oder Stelle übermittelt werden, gem. § 78 SGB X der Zweckbindung unterliegen: Sie dürfen lediglich zu den Zwecken verarbeitet werden, zu denen die Daten überlassen wurden.

[61] OLG Hamburg, Beschl. V. 29.09.2021 – 3 U 148/20
[62] https://www.kbv.de/media/sp/Anlage_31b_Videosprechstunde.pdf (zuletzt abgerufen am 08.04.2022)
[63] Vgl. § 12 SGB I, §§ 18 bis 29 SGB I

Übermittelt ein Sozialleistungsträger Sozialdaten an einen nicht-öffentlichen Rechtsträger, muss der empfangende nicht-öffentliche Rechtsträger vertraglich auf das Sozialgeheimnis verpflichtet werden.[64]

Die Verarbeitung von Sozialdaten im Auftrag wird in § 80 SGB X geregelt. Ein besonderes Augenmerk ist in diesem Zusammenhang auf § 80 Abs. 2 SGB X zu richten. Dort wird gesetzlich klargestellt, dass eine Verarbeitung von Sozialdaten im Auftrag nicht in unsicheren Drittstaaten stattfinden darf. Eine Datenverarbeitung kann demnach nur in der EU, in den Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum sowie in der Schweiz – vgl. § 35 Abs. 7 SGB I (neu) – und in einem Staat, für den ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO vorliegt, vorgenommen werden. Im Zweifel sollte die Ablage von sensitiven Daten ohnehin ausnahmslos verschlüsselt erfolgen.

Das Sozialgeheimnis verpflichtet in erster Linie die Sozialleistungsträger wie Krankenkassen, Jugend- oder Sozialämter, Renten- oder Unfallversicherungsträger, aber auch Verbände der Leistungsträger, die im Sozialgesetzbuch genannten öffentlich-rechtlichen Vereinigungen, die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist, oder die Zollverwaltung, soweit sie Aufgaben nach dem Schwarzarbeitsbekämpfungsgesetz wahrnimmt.

Krankenhausgesetzgebung

Obwohl die Neufassung des § 203 StGB ggf. eine Verarbeitung von Patientendaten in der Cloud ermöglicht, stehen diesem Vorhaben spezialgesetzliche Regelungen entgegen. So gab es je nach Bundesland Einschränkungen oder gar Verbote beim Einsatz externer Dienstleister. In Bayern war dies nur im Verbund durch andere Krankenhäuser möglich, z. B. mit Betrieb eines gemeinsamen Serverraums.[65]

Im Juni 2022 wurde das Bayerische Krankenhausgesetz (BayKrG) reformiert, um sich Cloud-Services und anderen Formen von Outsourcing zu öffnen. Nunmehr können die Kliniken im Freistaat nahezu uneingeschränkt moderne digitale Datenspeicher- und Verarbeitungslösungen von Cloud-Services nutzen, sofern diese sich mit der DSGVO vereinbaren lassen. Dazu heißt es in Absatz 6:

> *„Im Anwendungsbereich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), insbesondere Art. 28 DSGVO (Auftragsverarbeiter) und Art. 32 DSGVO (Sicherheit der Verarbeitung), sind besondere Schutzmaßnahmen technischer und organisatorischer Art zu treffen, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können."*[66]

Lange blieb die Speicherung und Verarbeitung patientenbezogener medizinischer Daten in der Cloud in einigen Bundesländern verwehrt. Nach Lockerungen in Berlin und Bayern dürften auch andere Bundesländer nachziehen, sofern dies noch nicht geschehen ist.

Telekommunikationsgesetz

Ein Arbeit- bzw. Dienstgeber, der geschäftsmäßig Telekommunikationsdienste anbietet, ist) zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Eine Verletzung des Fernmeldegeheimnisses ist nach § 206 Strafgesetzbuch (StGB) strafbar. Bis zum 30. November 2021 war das Fernmeldegeheimnis in § 88 Telekommunikationsgesetzt (TKG) geregelt. Zum 1. Dezember 2021 trat ein neues Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) in Kraft. Eine grundlegende Modernisierung des TKG war notwendig geworden, um u. a. die Rechtsunsicherheiten, die durch das bisherige Nebeneinander von DSGVO, TMG und TKG entstanden waren, aufzulösen. Die Datenschutzbestimmungen von TKG und TMG wurden hierzu in einem Gesetz zusammengefasst.

[64] Siehe § 78 Abs. 1 S. 2 SGB X
[65] https://www.lda.bayern.de/media/info_kh_leitfaden.pdf ab Seite 7, zuletzt abgerufen am 12.09.2022
[66] BayKrG, Art. 27, Absatz 6

Ziel des TTDSG war also die erforderliche Anpassung der Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) an die Datenschutz-Grundverordnung (DSGVO) sowie die – bereits lange ausstehende – Umsetzung der ePrivacy-Richtlinie (RiLi 2002/58/EG in der durch die RiLi 2009/136/EG geänderten Fassung). Teil 2 (§§ 3 bis 18) des TTDSG enthält die Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre in der Telekommunikation. Die Bestimmungen zum Fernmeldegeheimnis aus § 88 TKG-alt wurden in § 3 TTDSG überführt.

§ 2 Abs. 1 TTDSG bestimmt, dass zunächst die Begriffsbestimmungen des Telekommunikationsgesetzes auch für TTDSG gelten, soweit in § 2 Abs. TTDSG keine abweichende Begriffsbestimmung getroffen wird. Insofern hat es der Gesetzgeber versäumt, für die seit Jahren in Streit stehende Frage, ob er der Arbeit- resp. Dienstgeber als Diensteanbieter von Telekommunikationsdiensten anzusehen ist, eine Klärung herbeizuführen.

Umfang und Bedeutung des neuen TTDSG

Nach § 3 Abs. 1 TTDSG unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Wer zur Achtung des Fernmeldegeheimnisses nach verpflichtet ist, regelt § 3 Abs. 2 TTDSG. Demnach gehören hierzu Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten (vgl. § 3 Abs. 2 S. 1 Nr. 2 TTDSG). An diese Voraussetzung sind nur geringe Anforderungen zu stellen. Von Geschäftsmäßigkeit ist auszugehen, wenn ein nachhaltiges Angebot für Dritte mit oder ohne Gewinnerzielungsabsicht vorliegt.[67] Da in der neuen Fassung diese Trennung aufgehoben und die Entgeltlichkeit eine Voraussetzung ist, kommt es auf das Vorliegen eines „geschäftsmäßigen" Telekommunikationsdienstes aber wohl nicht (mehr) an[68].

Soweit bekannt, haben bisher allerdings weder der Bundesgerichtshof noch das Bundesarbeitsgericht abschließend darüber entschieden, ob ein Arbeit- resp. Dienstgeber, der seinen Mitarbeitenden die private E-Mail und/oder Internet-Nutzung von am Arbeitsplatz erlaubt, geschäftsmäßig Dienste i. S. d. TKG anbietet.[69] Im Rahmen der bisherigen Rechtslage empfiehlt es sich demnach den Arbeit- bzw. Dienstgeber als einen geschäftsmäßigen Anbieter einzustufen, sofern dieser die private Nutzung der betrieblichen Kommunikationsmittel erlaubt und diese seinen Mitarbeitenden für private Zwecke zur Verfügung stellt.

Neben der grundsätzlichen Beteiligung der Mitarbeitervertretung bei der Einführung von technischen Einrichtungen muss sich demnach auch mit der Frage bzgl. Wahrung des Fernmeldegeheimnisses auseinandergesetzt werden, durch welches insbesondere Telekommunikationsinhalt und -teilnehmer geschützt sind. Der Gesetzgeber ging in der Vergangenheit an verschiedenen Stellen davon aus, dass der Arbeitgeber TK-Anbieter wird, wenn er sich entscheidet, die Privatnutzung zu gestatten.[70] Und auch die Datenschutzaufsichtsbehörden des Bundes und der Länder positionieren sich in ihrer Orientierungshilfe aus dem Jahr 2016[71] eindeutig:

> *„Nach Auffassung der Aufsichtsbehörden ist der Arbeitgeber jedenfalls dann Telekommunikationsdienste- bzw. Telemediendienste-Anbieter, sobald er die private Nutzung von Internet- und IT-Infrastruktur durch die Mitarbeiter zulässt."*

Eine Begründung für diese Einschätzung geben die Aufsichtsbehörden leider nicht mit an die Hand. Es wird lediglich auf den Wortlaut des § 3 Nr. 6 TKG-alt verwiesen. Gerichte erteilten der Auffassung der Aufsichtsbehörden bisher überwiegend eine klare Absage und begründen[72] dies u. a. damit, dass der Arbeitgeber nicht geschäftsmäßig Telekommunikationsdienstleistungen erbringt, wenn er seinen

[67] Geppert/Schütz/Eckhardt, Beck'scher TKG-Kommentar, 4. Aufl. (2013), TKG § 111 Rn. 10.
[68] Rossow: Arbeitgeber und das Fernmeldegeheimnis nach dem TTDSG, DuD, S. 93 (95), 2/2022
[69] Legaldefinition siehe § 3 Nr. 6 TKG
[70] BT-Drucks. 17/4230 S. 43, http://dip21.bundestag.de/dip21/btd/17/042/1704230.pdf, zuletzt abgerufen am 15.01.2021
[71] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/OH_E-Mail_Internet_Arbeitsplatz.pdf
[72] Vgl. etwa LAG Berlin-Brandenburg, Urteil vom 14.01.2016 - 5 Sa 657/15

Mitarbeitern die private Nutzung der betrieblichen Kommunikationsmittel gestattet. Es fehle an dem Angebot von Telekommunikation, welches an außerhalb der Sphäre des Diensteanbieters liegende Dritte gerichtet ist.

Doch ergehen auch weithin anderslautende Entscheidungen, wie bspw. das Urteil des LAG Hessen[73], Die Kammer betont in ihrer Urteilsbegründung, dass der Arbeitgeber als Diensteanbieter i. S. d. § 3 Nr. 6 TKG-alt anzusehen ist, wenn er das Versenden privater E-Mails erlaubt.[74]

Das Problem steckt für den vermeintlichen Diensteanbieter (Arbeit-/Dienstgeber) nunmehr im Detail. Unterfällt er – nach dem Willen der Aufsichtsbehörden – dem Anwendungsbereich des TKG resp. des TTDSG, so ist es ihm gem. § 3 Abs. 1 TTDSG untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Eine Protokollierung von Telekommunikationsdaten zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zu Abrechnungszwecken bleibt, soweit erforderlich, zulässig. Eine darüber hinaus gehende Kontrolle wäre jedoch unzulässig.

Möglichkeiten zur Gestaltung in der Praxis

Vereinfacht dargestellt ist dem Arbeit- bzw. Dienstgeber damit bereits ein Zugriff auf das E-Mail-Postfach des Mitarbeitenden grundsätzlich verwehrt, da bei gleichzeitig privater und dienstlicher Nutzung die Inhalte der Kommunikation (hier E-Mails) durch das Fernmeldegeheimnis geschützt sind. Anders gewendet machte der Dienst-/Arbeitgeber sich wegen Verletzung des Post- und Fernmeldegeheimnisses strafbar, wenn er bspw. bei ungeplanter Abwesenheit eines Mitarbeitenden einfach so auf das E-Mail-Postfach des Mitarbeitenden zugreifen würde – und dies selbst dann, wenn seine Absichten hehrer Natur sind und er lediglich seinen Geschäftsbetrieb aufrechterhalten möchte.

Der bisherige Königsweg aus diesem Dilemma, will man die private Nutzung nicht per se verbieten, war der Abschluss einer Dienst- bzw. Betriebsvereinbarung mit den Arbeitnehmervertretern und eine (schriftliche) Einwilligung der Mitarbeitenden, mittels welcher die private Nutzung am Arbeitsplatz unter eine angemessene technische und organisatorische Kontrolle gestellt werden kann. Verweigert der Arbeitnehmer seine Zustimmung, muss er die private Nutzung von bspw. E-Mail und Internet am Arbeitsplatz unterlassen.

Das Beschreiten des Königswegs kann sich jedoch als Bärendienst erweisen: Das TTDSG stellt die Kenntnisnahme von Inhalten aus Telekommunikationsvorgängen für Diensteanbieter unter Strafe. Der Arbeit- bzw. Dienstgeber (als zwangsweiser Diensteanbieter) versucht sich frei zu zeichnen, indem seine Mitarbeitenden einwilligen, auf diesen gesetzlichen Schutz an dieser Stelle zu verzichten. Dies kann nicht im Sinne der Gesetzgebung sein. Eine höchstrichterliche oder gesetzliche Klärung bzgl. der Frage, ob ein Arbeit- bzw. Dienstgeber in den Anwendungsbereich fällt, ist wünschenswert und längst überfällig. Die ersehnte Hoffnung, das mit Einführung des TTDSG die Frage, ob der Dienst- bzw. Arbeitgeber Diensteanbieter ist, einer Klärung herbeigeführt würde, wurde leider nicht erfüllt.

Aus praktischer Sicht bleibt daher vor allem von Bedeutung, eine Privatnutzung betrieblicher Kommunikationsmittel nicht einfach zu dulden, sondern, wenn eine solche erlaubt werden soll, dies explizit zu tun und zugleich klare „Spielregeln“ und Kontrollmechanismen aufzustellen, z.B. per Betriebs-/Dienstvereinbarung und hierauf Bezug nehmender Einwilligungen der einzelnen Mitarbeitenden.[75]

[73] LAG Hessen Urt. v. 21.9.2018 – 10 Sa 601/18
[74] LAG Hessen: Einsichtnahme des Arbeitgebers in die – auch private – E-Mail-Korrespondenz des Arbeitnehmers, CR 2019, 811
[75] GDD-Praxishilfe: Das neue Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) im Überblick, Stand Juni 2021, S. 8

Elektronische Buchführung und Aufbewahrung

Die klassischen Aufbewahrungsfristen für Handels-, Geschäftsbriefe, Jahresabschlüsse usw. ergeben sich aus § 257 Handelsgesetzbuch (HGB) bzw. § 147 Abgabenordnung (AO). Daneben gibt es selbstverständlich weitere zu beachtende Vorschriften (exemplarisch GoB, GoBD, BetrAVG) und ganz grundsätzlich ist die generelle regelmäßige Frist (Verjährung) aus § 195 Bürgerliches Gesetzbuch (BGB) zu beachten.

Die Aufbewahrung handels- und steuerrechtlicher Dokumente ist via M365 (SharePoint Online und Exchange) in digitaler Form möglich. In jedem Fall Beachtung finden sollten dabei die Regelungen der Abgabenordung (AO). Nach § 146 Abs. 2 AO dürfen steuerlich relevante Daten grundsätzlich nur im Inland aufbewahrt und geführt werden. Bücher und die sonst erforderlichen Aufzeichnungen sind somit im Geltungsbereich der Bundesrepublik Deutschland zu führen und aufzubewahren.

Abweichend kann die zuständige Finanzbehörde auf schriftlichen Antrag des Steuerpflichtigen, und unter in § 146 Abs. 2b AO aufgeführten Voraussetzungen, bewilligen, dass elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb des Geltungsbereichs der Bundesrepublik geführt und aufbewahrt werden können.

In welchem Umfang Dienste von M365 und die damit verbundenen Speicherorte in den Kontext „steuerlich relevante Daten“ fallen, ist zu klären. Im Zweifel ist dies vor Nutzung von Speicherlösungen im Ausland beim jeweiligen Finanzamt zu erfragen.

Elektronische Personalakten

Es finden sich im Gesetz zwar keine konkreten Regelungen zum Führen einer Personalakte, gleichwohl sind im Umgang mit elektronischen Personalakten zahlreiche rechtliche Aspekte zu beachten. Hierzu zählen insbesondere das Persönlichkeitsrecht der Mitarbeitenden, der Datenschutz, die technischen und organisatorischen Maßnahmen und ggf. zu beachtende Beteiligungsrechte der Mitarbeitervertretungen.

Der Personalakte ist eine Vielzahl von personenbezogenen Daten von Mitarbeitenden immanent. Dazu gehören regelmäßig nicht nur Name, Anschrift, Lebenslauf und Zeugnisse, sondern oftmals auch besonders sensible Daten, wie Gesundheitsdaten. Dieser Umstand erfordert besondere Voraussetzungen bei der Speicherung und Verarbeitung von Personalakten auf elektronischem Wege:

- Berechtigungs- und Rollenkonzept für den Zugriff,
- Ausreichender Schutz vor unbefugtem Zugriff,
- Einwilligung der Mitarbeitenden zur Speicherung ihrer Daten,
- Möglichkeit der Einsichtnahme von Mitarbeitenden in ihre Personalakte.

Das Vorhalten von elektronischen Personalkaten ist auch mittels M365 grundsätzlich möglich. So können etwa in SharePoint die rechtlichen und die technisch-organisatorischen Anforderungen durchaus erfüllt werden: Dokumente werden versioniert, mit Metadaten wie Ersteller, Schlagworten, Erstellungs- und Veränderungsdatum versehen und gespeichert. Alternativ gibt es Drittanbieter, die eigene Applikationen für die Elektronische Personalakte als Integration in M365 anbieten.

Ausweitung Standarddatenschutzklauseln

Sofern der Lizenzvertrag für die Enterprise Cloud Services von Microsoft mit einer zentralen Gesellschaft – etwa dem Shared Service Center für die IT im Konzern oder Verbund, abgeschlossen werden – sollten alle nutzenden Gesellschaften im Konzern bzw. Verbund die Auftragsverarbeitungsvereinbarung und die EU-Standardvertragsklauseln unterzeichnen. Aus Sicht der Datenschutzaufsichtsbehörden sind diese allesamt Verantwortliche im datenschutzrechtlichen Sinne. Zur Erfüllung dieser gesetzlichen Vorgabe bietet Microsoft ebenfalls eine Zusatzvereinbarung an.

IV. Auftragsverarbeitung, Unterauftragnehmer und Drittanbieter

Hat Microsoft Eigeninteresse an den in M365 gespeicherten Daten?

Worin besteht der Unterschied zwischen Auftragsverarbeitung und einer Gemeinsamen Verantwortlichkeit (Joint Controllership)?

Auftragsverarbeitung	Bei der Auftragsverarbeitung (AV) verarbeitet ein Dienstleister (Auftragnehmer) personenbezogene Daten der Organisation (Auftraggeber) im Auftrag. Mittels eines Vertrags zur Auftragsverarbeitung (AV-Vertrag, DPA) werden die Rechte und Pflichten beider Parteien geregelt. Der Auftragsverarbeiter hat an den zu verarbeitenden Daten kein eigenes Interesse und verarbeitet diese nicht zu eigenen Zwecken weiter, sondern stets nach Vorgabe des Auftraggebers.
Gemeinsame Verantwortlichkeit	Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. [76] Wichtigste Voraussetzung für die gemeinsame Verantwortlichkeit ist also die gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.

Microsoft verarbeitet Daten als Auftragsverarbeiter und darüber hinaus Daten zu „legitimen Geschäftszwecken“ (Eigeninteresse) als unabhängiger Datenverantwortlicher. Für die Zwecke des Data Processing Agreement (DPA) umfassen legitime Geschäftstätigkeiten von Microsoft die folgenden Aktivitäten:[77]

- Abrechnungs- und Kontoverwaltung
- Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives)
- interne Berichterstattung und Geschäftsmodellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie)
- Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft selbst oder Microsoft-Produkte betreffen könnten
- Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz
- Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen

Ob die von Microsoft aufgeführten „legitimen Geschäftstätigkeiten“ mit der Rolle von Microsoft als Auftragsverarbeiter vereinbar sind oder nicht, kann ohne zusätzliche Informationen nicht vollends beurteilt werden. Hierfür wäre es notwendig zu erfahren, welche Daten explizit von Microsoft zu den oben aufgeführten Zwecken in Eigenregie verarbeitet werden.

Ob für die „legitimen Geschäftszwecke” der AV-Vertrag ausreichend ist, ist darüber hinaus fraglich. Unter Umständen wäre hierfür ein Vertrag über die gemeinsame Verantwortlichkeit bzw. Joint-Controllership-Vertrag[78] notwendig, für den nach Kenntnisstand der Autoren bisher keine Vorlage von Microsoft vorliegt.

[76] Siehe Art. 26 Abs. 1 Satz 1 DSGVO | § 29 Abs. 1 Satz 1 DSG-EKD | § 28 Abs. 1 Satz 1 KDG
Siehe Datenschutznachtrag zu den Produkten und Services von Microsoft [DPA] Letzte Aktualisierung: 15. September 2021, Seite 6

[78] Nach Aussage von Microsoft werden die Daten für „legitime Geschäftszwecke“ von Microsoft selbst erhoben, sodass aus Sicht von Microsoft keine gemeinsame Verantwortung vorliegt.

Dass es sich um eine teilweise gemeinsame Verantwortlichkeit handeln kann, wird aus der folgenden Formulierung ersichtlich:

> *„Soweit Microsoft personenbezogene Daten, die der DSGVO unterliegen, für Geschäftstätigkeiten im Zusammenhang mit der Bereitstellung der Produkte und Services an den Kunden nutzt oder anderweitig verarbeitet, wird Microsoft für diese Nutzung die Pflichten eines unabhängigen Datenverantwortlichen gemäß der DSGVO erfüllen."*[79]

Im Herbst 2022 wird ein überarbeitetes Data Protection Agreement erwartet, dass zur Freigabe der vorliegenden Version dieses Papiers noch nicht vorlag.

Welche Anforderungen gilt es für Dienstleister von Microsoft zu beachten?

Die datenschutzrechtlichen Anforderungen gelten nicht nur bei der Auftragsverarbeitung durch einen Dienstleister wie Microsoft, sondern müssen auch von eingesetzten Unterauftragsnehmern des Dienstleisters eingehalten werden.

Microsoft arbeitet selbst weltweit mit einer großen Anzahl an "Unterauftragsverarbeitern" zusammen. Im Microsoft Trust-Center[80] kann eine aktuelle Liste der Unterauftragsverarbeiter für Microsoft Online Services heruntergeladen werden.

Die datenschutzrechtlichen Regelungen, die für die Übermittlung und Verarbeitung von personenbezogenen Daten an und durch Microsoft gelten, sind ebenfalls beim Einsatz von Unterauftragsverarbeitern notwendig. Datenschutzrechtlich verantwortlich bleibt immer die Organisation als Auftraggeber, die sich für Microsoft-Dienste entschieden hat. Daher wird empfohlen, die Unterauftragsverarbeiter von Microsoft regelmäßig zu prüfen und die Rechtmäßigkeit einer Übermittlung und Verarbeitung der Daten kritisch zu hinterfragen.

Microsoft führt selbst regelmäßig Audits und Kontrollen bei seinen Dienstleistern durch und verpflichtet sich, die Einhaltung der in dem DPA beschriebenen Verpflichtungen von Microsoft bei seinen Unterauftragsverarbeitern durchzusetzen.

Was ist bei Add-ons zu berücksichtigen?

Add-ons für Microsoft 365 von Drittanbietern sind wie eigenständige Software-Lösungen vor ihrem Einsatz in Hinblick auf Datenschutz & Compliance zu prüfen.

Einzelne M365-Anwendungen bieten die Möglichkeit, Erweiterungen einzubinden, so genannte Add-ons. Insbesondere Microsoft Teams ist von vorneherein so aufgebaut, dass andere Anwendungen des M365-Pakets integriert werden können, z. B. ein Kanal-eigenes Kanban-Board im Planner oder Notizen in OneNote.

Darüber hinaus können Apps integriert werden, die nicht im M365-Umfang enthalten sind. Sie sind in zwei Kategorien zu unterteilen und jeweils gesondert zu betrachten:

---

[79] Siehe Datenschutznachtrag zu den Produkten und Services von Microsoft [DPA] Letzte Aktualisierung: 15. September 2021, Seite 7

[80] Siehe https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List, zuletzt abgerufen am 12.09.2022

Microsoft-Apps

Diese Apps werden durch Microsoft innerhalb der Azure-Cloud-Umgebung bereitgestellt und unterliegen damit im Wesentlichen denselben Datenschutz- und Compliance-Bedingungen, die auch für die Nutzung von M365 gelten (siehe hierzu „Verbundene Dienste“ auf Seite 18).[81]

Third-Party-Apps

Außerdem können Apps von Drittanbietern in Teams eingebunden werden.[82] Ein Anwendungsbeispiel wäre ein Tool zum gemeinsamen Sammeln und Organisieren von Ideen, das in seinen Funktionen über die Möglichkeiten des standardmäßig integrierten Whiteboards hinausgeht, in dem sich etwa Mindmaps erstellen lassen.

Solche Third-Party-Apps sind – trotz ihrer Einbindung in die Teams-Oberfläche – unter Datenschutz- und Compliance-Gesichtspunkten wie eigenständige Software-Lösungen zu betrachten, die ins System eingebunden werden sollen. Das bedeutet, dass die lizenzrechtlichen Bedingungen genau zu prüfen und auch die Wege der Datenübertragung sowie die Orte der Speicherung im Einzelfall zu betrachten sind.

Hier wird regelmäßig ein zusätzlicher Vertrag zur Auftragsverarbeitung zu schließen und dieser ggf. um Standarddatenschutzklauseln + TIA und ergänzender Maßnahmen/Garantien zu ergänzen sein, falls die Anwendung in Drittländer Daten überträgt.

Meist herrscht bei den Anbietern jedoch eine gewisse Awareness für die Anforderungen aus dem europäischen Datenschutzrecht vor, so dass man in der Regel mühelos die erforderlichen Angaben zu TOM sowie Vorlagen für ein Data Processing Agreement (DPA) findet. Zudem handelt es sich häufig um Start-up-Unternehmen, die eine offene Kommunikation mit (potenziellen) Kunden pflegen.

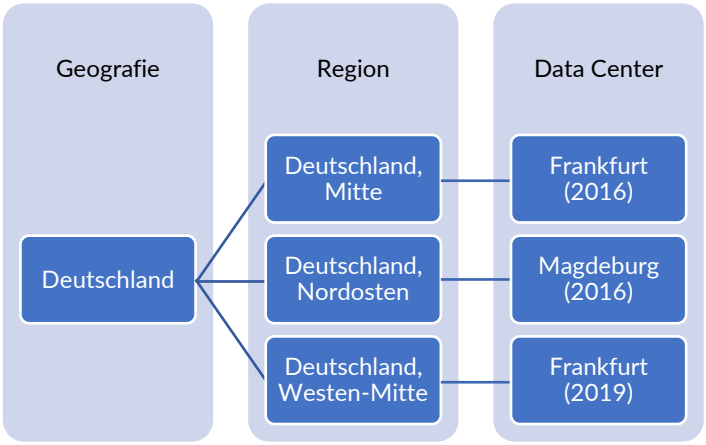
[81] https://docs.microsoft.com/de-de/microsoftteams/teams-add-on-licensing/microsoft-teams-add-on-licensing?tabs=small-business, zuletzt aufgerufen am 12.09.2022
[82] https://docs.microsoft.com/de-de/microsoftteams/purchase-third-party-apps, zuletzt aufgerufen am 14.07.2022

V. Microsoft 365 und Drittlandtransfer

Werden beim Einsatz von M365 personenbezogene Daten in Länder außerhalb Europas wie z. B. die USA übermittelt?

Bei Nutzung von Microsoft 365 werden grundsätzlich personenbezogene Daten in ein Drittland (i.d.R. die USA) übermittelt. Die Speicherung von Daten erfolgt überwiegend in Europa, für die Nutzung vieler Dienste sind Stand Sommer 2022 weiterhin internationale Datentransfers erforderlich.

Um die Übermittlung und Speicherung von Daten innerhalb der M365 Struktur nachvollziehen zu können, lohnt ein Blick auf die unterschiedlichen Begriffsdefinitionen[83]:



Geografien (Geography):

Eine Geografie hat typischerweise zwei oder mehr Regionen. Geografien werden fehlertolerant ausgelegt, um den Ausfall einer kompletten Region kompensieren zu können. Beispiele für Geografien sind Deutschland und Frankreich (jeweils eine eigene Geografie).

Regionen (Region):

Eine Region besteht aus einem oder mehreren Rechenzentren innerhalb eines Latenzradius. Ein Beispiel für eine Region ist Deutschland, Westen-Mitte mit dem Rechenzentrum in Frankfurt.

Verfügbarkeitszonen (Availability Zones):

Verfügbarkeitszonen sind physisch getrennte Standorte innerhalb einer Region und bestehen jeweils aus einem oder mehreren Rechenzentren. Mithilfe von Azure Verfügbarkeitszonen können weitreichende Szenarien zum IT-Notfallmanagement realisiert werden. Am Standort Frankfurt stehen gegenwärtig drei Verfügbarkeitszonen bereit.[84]

Grundsätzlich können Kunden die „Core-Onlinedienste" von Microsoft derart konfigurieren, dass diese in einem Rechenzentrum innerhalb einer Geografie bereitgestellt werden.[85] Infolgedessen speichert Microsoft die Kundendaten „at rest" (gespeicherte Daten, also vergleichbar mit Dateien auf einer Festplatte) innerhalb dieser Geografie, bspw. innerhalb von Deutschland, Westen-Mitte.

[83] https://azure.microsoft.com/de-de/explore/global-infrastructure/, zuletzt abgerufen am 12.09.2022
[84] Azure-Geografien, https://azure.microsoft.com/de-de/global-infrastructure/geographies, abgerufen am 07.04.2022.
[85] Bei M365 richtet sich die Region nach der Rechnungsadresse des Tenants.

Zu unterscheiden ist dies von der Verarbeitung von Daten: Einzelne Funktionen in M365 stehen möglicherweise nur außerhalb der gewählten Geografie bereit, so dass die Daten für die Verarbeitung in ein anderes Land übermittelt werden müssen (data in transit). Je nach Dienst kann eine Übermittlung in die USA erforderlich werden, wenn die Verarbeitung selbst nicht in Europa stattfinden kann.[86] Auf den Transportwegen erfolgt eine Verschlüsselung und nach der Verarbeitung werden die Daten wieder in der gewählten Geografie gespeichert.

Stand Sommer 2022 werden die Daten von Kundenkonten aus Deutschland überwiegend in Deutschland oder der Europäischen Union gespeichert. Bei nur wenigen Diensten erfolgt die Speicherung der Daten (data at rest) außerhalb der EU[87]. Sway und Viva Insights sind vergleichsweise selten im Einsatz.

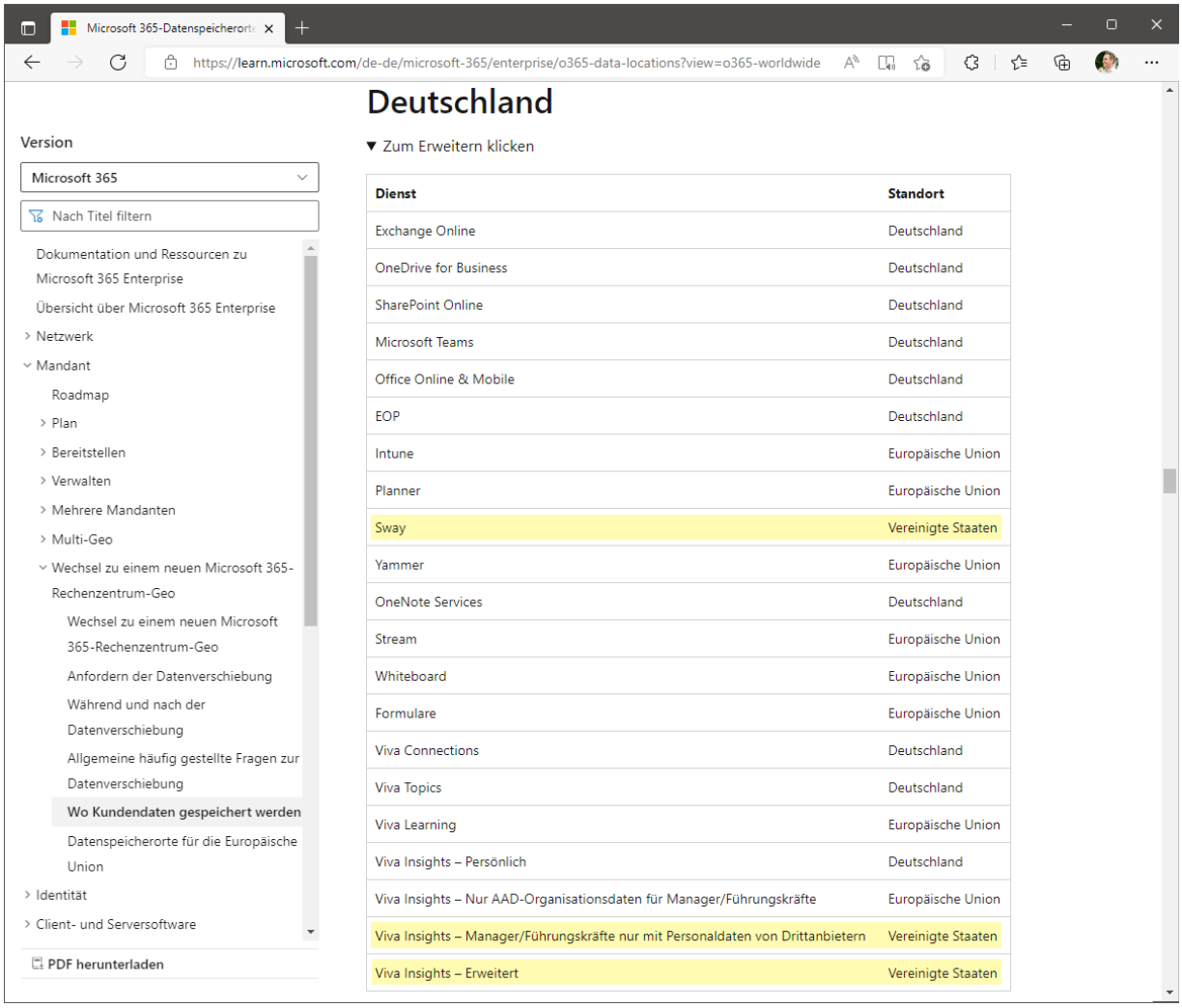


Abbildung 2: Liste der Standorte, wo Kundendaten für einen Tenant aus Deutschland gespeichert werden (data at rest)[88]

[86] https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide#where-eu-data-is-computed, zuletzt abgerufen am 26.01.2021
[87] https://learn.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide, zuletzt abgerufen für einen deutschen Tenant am 12.09.2022
[88] https://learn.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide#data-center-locations, zuletzt abgerufen am 12.09.2022

Etwas versteckt und nur über Umwege mit Hilfe von PowerShell ermittelbar, können die Server-Standorte der einzelnen Dienste im Microsoft- bzw. Office 365-Umfeld abgefragt werden.

Hier zeigt sich ein gänzlich anderes Bild: Stand Sommer 2022 werden viele Dienste für ein deutsches Microsoft 365-Kundenkonto aus den USA heraus betrieben. In der Liste der Funktionen finden sich weit verbreitete Funktionen wie Windows Defender, Microsoft Office, Office Forms, ToDo oder auch die Whiteboard-Funktion in Microsoft Teams.

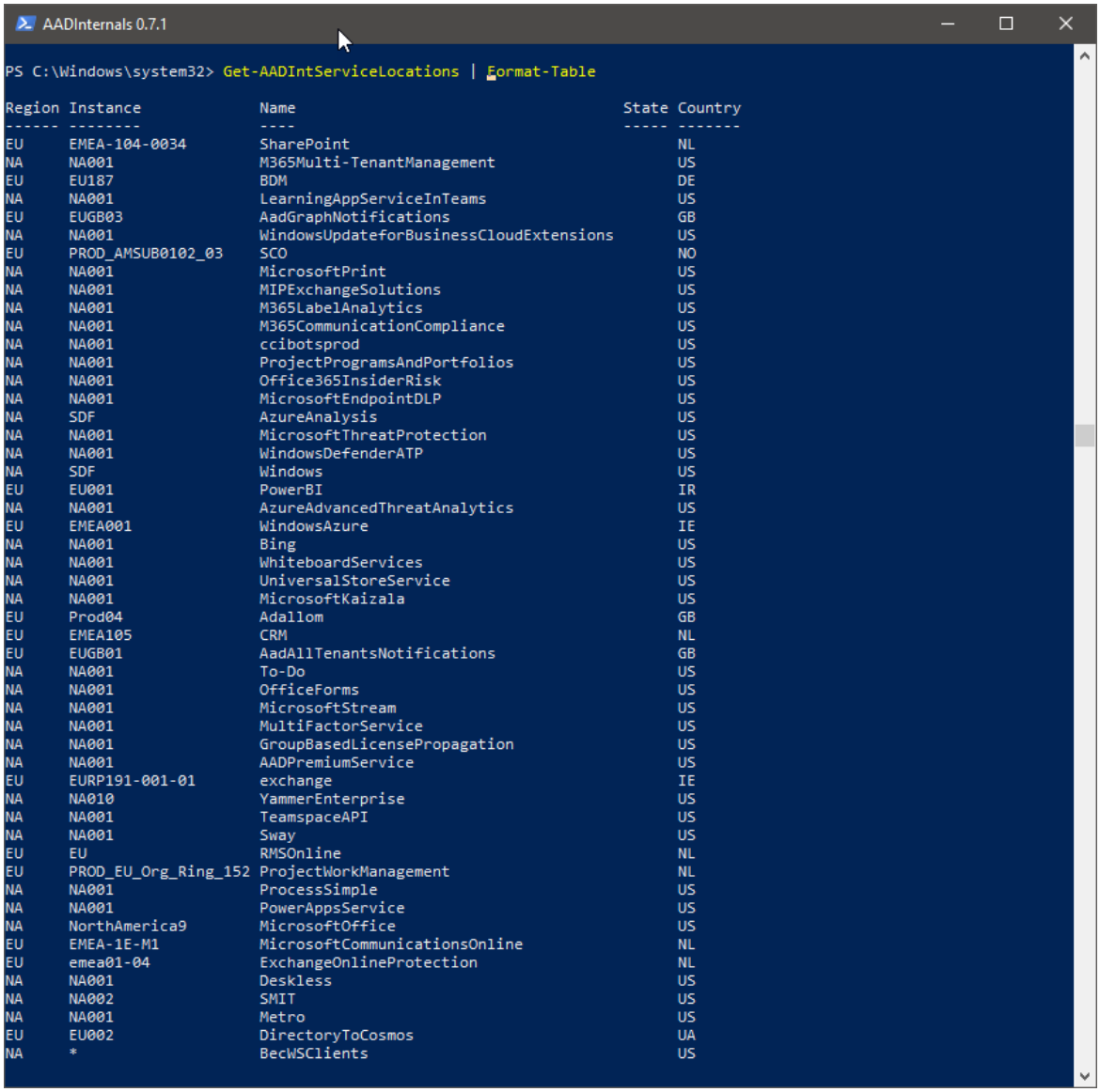


Abbildung 3: Abfrage der Server-Standorte von Microsoft 365-Diensten für ein deutsches Kundenkonto[89]

Für einen deutschen Tenant werden also bei Zugriff auf einige weit verbreitete Funktionen der Microsoft 365-Suite Kundendaten in die USA übertragen und beim Speichern der Daten erfolgt der Transfer zurück nach Deutschland. Stand Sommer 2022 müssen Kunden also zumindest zeitweise eine Übermittlung und das Zwischenspeichern ihrer Daten außerhalb Europas für kurze Zeit akzeptieren.

[89] Get-AADIntServiceLocations (weitere Skripte/Funktionen müssen zuvor geladen werden), zuletzt abgerufen am 12.09.2022

Die Liste der Geografien wird von Microsoft stetig erweitert und ausdifferenziert, da auch die Anzahl der Rechenzentren wächst. Während für deutsche Kunden die Auswahl der Geografien bis vor einigen Jahren aus „Europe“ mit den Regionen Irland und Niederlande bestand, lassen sich Geografien mittlerweile deutlich eingegrenzter auswählen. So werden unter anderem alle Rechenzentren in Deutschland (genauer: Frankfurt, Magdeburg) unter der Geografie „Deutschland“ zusammengefasst.

Die Wahl einer Geografie und nicht etwa nur einer Region ist sinnvoll, da so der mögliche Ausfall einer Region ohne Einbußen hinsichtlich der Verfügbarkeit kompensiert werden kann. Eine Region besteht wiederum meist aus mehreren physisch getrennten Rechenzentren (Verfügbarkeitszonen), sodass auch der temporäre Ausfall einer Verfügbarkeitszone kompensiert werden kann. Die vollständige Liste aller Geografien und Regionen kann der Microsoft-Webseite entnommen werden.[90]

Bei einigen Diensten und Funktionen haben Kunden unter Umständen jedoch nicht die Möglichkeit, die Bereitstellung ihrer Daten in einer bestimmen Geografie und insbesondere außerhalb der USA auszuwählen, wie die Abfrage der Serverstandorte zeigt. Beispielsweise ist eine Übermittlung von Daten unter anderem bei der Nutzung der Multi-Faktor-Authentifizierung mittels SMS/Telefonanruf (MfA) sowie bei Support-Anfragen notwendig, da die Serviceprovider in den USA sitzen. Ein weiteres Beispiel kann der 3rd-Level-Support sein, der – je nach Fallkonstellation – auch direkt aus den USA oder einem anderen Drittland heraus erbracht wird (Follow-the-Sun-Prinzip).[91]

Ausblick: Einführung des EU Data Boundary ab Ende 2022

Im Mai 2021 hat Microsoft angekündigt, im Rahmen des Programms „EU Data Boundary for the Microsoft Cloud“ bis Ende 2022 die technischen Voraussetzungen dafür zu schaffen, dass Daten gar nicht mehr außerhalb der EU verarbeitet werden müssen.[92] Darüber hinaus soll Support-, Sicherheits- und Wartungspersonal in Europa aufgestockt werden. Der Zugriff auf Support-Daten durch außereuropäische Standorte (z. B. zur Analyse von Fehlern) soll nur noch in sehr engen Grenzen möglich sein und durch eine Virtual Desktop Infrastructure (VDI) bzw. Screen-Rendering geschützt werden.

Diese Ankündigung wurde in Branchenkreisen sehr begrüßt und dürfte die vorgenannten transatlantischen Datenströme in vielen Fällen überflüssig machen. Nach eigenen Angaben von Microsoft werden sodann nicht nur die Kerndienste, sondern sämtliche eigenen Applikationen und Tools von Microsoft in Europa vorgehalten; die europäische Datengrenze bliebe damit vollumfänglich ohne einen „geheimen Grenzübergang“ gewahrt.

Wenngleich die Initiative regulatorische Anforderungen besser erfüllen wird und den Bedürfnissen der europäischen Microsoft-Kunden entgegenkommt, wird die Problematik der Drittlandübermittlung durch US-Behördenzugriffe auf Basis des CLOUD-Acts auch durch das EU Data Boundary nicht aufgelöst.

[90] Azure-Geografien, https://azure.microsoft.com/de-de/global-infrastructure/geographies, Abruf am 07.04.2022.
[91] Damit Microsoft den technischen Support 24 Stunden am Tag, und an 7 Tagen die Woche gewährleisten kann, arbeiten die Service-Mitarbeiter an Standorten weltweit nach dem „Follow the Sun“-Prinzip: Der Support erfolgt von dort, wo es gerade Tag ist.
[92] EU Data Boundary for the Microsoft Cloud: A progress report, https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report, Abruf am 07.04.2022.

Ist die Übermittlung datenschutzrechtlich zulässig?

Die Übermittlung personenbezogener Daten in Drittländer, wie sie bei der Nutzung von M365 erfolgt, ist in der Regel nur möglich, wenn Garantien zum Schutz der Daten vorhanden sind. Nach Rechtsprechung des EuGH besteht in den USA kein gleichwertiges Schutzniveau, daher sind zusätzlich zu vertraglichen Regelungen wie in Standardvertragsklauseln weitere Maßnahmen erforderlich (z. B. Verschlüsselung).

DSGVO und Kirchengesetze zum Datenschutz verlangen, dass ein Vertrag zur Auftragsverarbeitung geschlossen wird, wenn personenbezogene Daten von externen Dienstleistern verarbeitet werden. Das ist bei der Nutzung von Cloud-Diensten wie M365 der Regelfall. Ist absehbar, dass personenbezogene Daten dabei die Europäische Union oder den Europäischen Wirtschaftsraum verlassen, sind die allgemeinen Grundsätze der Datenübermittlung[93] sowie Kapitel V DSGVO zu beachten.

Eine Übermittlung von personenbezogenen Daten an Drittländer ist demnach unter anderem zulässig, wenn ein angemessenes Datenschutzniveau[94] im Drittland besteht (festgestellt durch einen Angemessenheitsbeschluss der EU-Kommission). Nachdem für die Übermittlung von personenbezogenen Daten in die USA das sog. EU-US Privacy Shield im Juli 2020 durch den Europäischen Gerichtshof (EuGH) für unwirksam erklärt wurde und die Feststellung eines gleichwertigen Datenschutzniveaus für die USA vom EuGH explizit verneint wurde („Schrems II"),[95] bedarf es anderer geeigneter Garantien für die Datenübermittlung.

In diesem Fall werden als Rechtsgrundlage für die Übermittlung von personenbezogenen Daten in Drittstaaten oftmals Standarddatenschutzklauseln[96] (als Anlage eines AV-Vertrags) angeführt, häufig SCC abgekürzt (Standard Contractual Clauses). Im Zuge des Urteils bestätigte der EuGH die Wirksamkeit bzw. Anwendbarkeit der SCC als Rechtsinstrument für eine Drittlandübermittlung. Allerdings forderte der EuGH, dass der Datenexporteur in Hinblick auf die Übermittlung in ein „sicheres Drittland" zusätzlich eine Überprüfung inkl. Dokumentation vornimmt:

1. Erfassung aller auf Standarddatenschutzklauseln basierter Datentransfers
2. Faktensammlung zu den betroffenen Datenimporteuren
3. Faktensammlung zur Rechtsordnung im Drittland
4. Benchmark der relevanten Rechtsordnung Drittland vs. EU

Standarddatenschutzklauseln (SCC) & Transfer Impact Assessment (TIA)

In der Folge hat die Europäische Kommission überarbeitete SCC vorgelegt, die seit 27.09.2021 bindend sind und bis 26.12.2022 auch für Bestandsverträge nach alten SCC nachgerüstet werden müssen[97]. Hier entsteht vor allem Handlungsbedarf durch die Klauseln 14 und 15, nach denen zusätzliche Garantien des Datenimporteurs einzuholen und zu dokumentieren sind, um ein angemessenes Schutzniveau der personenbezogenen Daten im Drittland zu gewährleisten.

[93] Siehe Art. 44 DSGVO
[94] Art. 45 DSGVO, die aktuelle Liste der Länder mit Angemessenheitsbeschluss findet sich unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, zuletzt abgerufen am 06.01.2021
[95] Urteil ECLI:EU:C:2020:559, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first%E2%88%82=1&cid=10333140, Abruf am 08.04.2022.
[96] Siehe Art. 46 Abs. 2 lit. c) DSGVO
[97] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de, Abruf am 07.04.2022.

Zu diesem Zweck ist ein so genanntes „Transfer Impact Assessment“ (TIA) durchzuführen, um das Rechtsniveau im Drittland beurteilen zu können. Dieses muss dokumentiert werden und der Datenimporteur muss zusichern, dass er den Datenexporteur über Änderungen in Kenntnis setzt. Im Zentrum der Betrachtung eines TIA stehen die rechtlichen Voraussetzungen im Drittland, „die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten“.

Des Weiteren muss sich der Datenimporteur zu einem restriktiven Umgang mit Behördenersuchen verpflichten, das eine umfassende Transparenz gegenüber dem Datenexporteur und gegenüber betroffenen Personen umfasst, ferner die Ausschöpfung aller rechtlichen Mittel gegen die Erfüllung solcher Behördenersuchen sowie die Beschränkung der offenzulegenden Daten auf das zulässige Minimum.

Formale Vorgaben für eine TIA lassen sich den SCC nicht entnehmen und konkrete Arbeitshilfen auch von Seiten der Datenschutz-Fachverbände stehen größtenteils gegenwärtig noch aus.[98] Die vorzunehmende Risikobewertung lässt sich wohl am ehesten als eine Art reduzierte Datenschutz-Folgenabschätzung bezogen auf das Rechtsniveau im Drittland betrachten.

CLOUD Act

In diesem Kontext darf ein Blick auf den 2018 erlassenen CLOUD Act nicht fehlen.[99] Dieser wurde am 23. März 2018 vom US- Kongress verabschiedet und sollte eine neue Rechtsgrundlage für Herausgabeverlangen US-amerikanischer Gerichte bzgl. Informationen/Daten, die auf Servern außerhalb der USA gespeichert sind, darstellen.

Der erste Teil des CLOUD Acts verpflichtet US-amerikanische Firmen auf entsprechende Anordnung eines Gerichts Unterlagen und Daten herauszugeben, auch wenn sich diese außerhalb der USA befinden, soweit die Firma in Besitz dieser Unterlagen ist oder ein entsprechendes Zugriffs- bzw. Kontrollrecht hat. Wenn Server von Tochtergesellschaften im Ausland betrieben werden, ist dies der Fall.

Der Konflikt resp. Widerspruch zwischen europäischem Datenschutzrecht und dem CLOUD Act manifestiert sich auch gesetzlich in Art. 48 DSGVO.[100] Dieser regelt, dass ein derartiger Zugriff nur aufgrund eines Gerichtsurteils oder einer behördlichen Entscheidung eines Drittlands oder aufgrund einer internationalen Übereinkunft erfolgen darf. Anders gewendet bedarf es eines Rechtshilfeabkommens, um Unterlagen/Daten, die personenbezogene Informationen beinhalten, an Gerichte/Behörden in den USA zu übermitteln. Der CLOUD Act selbst sieht ein entsprechendes Abkommen – das bisher nicht besteht – aber nur in dem umgekehrten Fall vor, in dem Drittstaaten die Herausgabe von Unterlagen verlangen, die sich in den USA befinden.[101]

[98] Europäische Datenschutzausschuss (EDSA), Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de, Abruf am 08.04.2022; EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_de, Abruf am 08.04.2022; Stiftung Datenschutz, Internationale Datentransfers. Eine Handreichung, https://stiftungdatenschutz.org/fileadmin/Redaktion/PDF/Internationale_Datentransfers/RZ_SDS_Drittlands-Datentransfers_19112021.pdf, Abruf am 08.04.2022. Eine gute Übersicht und Auseinandersetzung mit den Maßnahmen siehe Hansen-Oest: Drittlandsverarbeitung in Zeiten von Schrems II“ in DSB 12/2020, S. 300.

[99] Clarifying Lawful Overseas Use of Data (CLOUD) Act; vgl. hierzu United States Department of Justice, CLOUD Act Resources, https://www.justice.gov/dag/cloudact, Abruf am 08.04.2022.

[100] Vgl. etwa Stellungnahme EDA: https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf, zuletzt abgerufen am 12.09.2022

[101] Ausführlich siehe Lejeune: Der US CLOUD Act: eine neue Rechtsgrundlage für den internationalen Datenzugriff?, ITRB 2018, S. 118 (S. 121)

Microsoft veröffentlicht regelmäßig Zahlen bezüglich Auskunftsbegehren aus CLOUD Act und deren Durchsetzung im Law Enforcement Requests Report[102] und hat im Dezember 2020 ein Kompendium[103] herausgebracht, in welchem sich auch mit dem CLOUD Act beschäftigt wird.

In der Diskussion um den CLOUD Act wird gerne übersehen, dass andere Staaten – auch in Europa – ihren Behörden vergleichbare Privilegien hinsichtlich der Einsichtnahme in personenbezogene Daten einräumen.

Nach § 110 Abs. 3 Strafprozessordnung (stopp) ist beispielsweise „die Durchsicht von elektronischen Speichermedien bei dem von der Durchsuchung Betroffenen zulässig. Diese Durchsicht darf auch auf hiervon räumlich getrennte Speichermedien erstreckt werden, soweit auf sie von dem elektronischen Speichermedium aus zugegriffen werden kann, wenn andernfalls der Verlust der gesuchten Daten zu befürchten ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden."

Two wrongs don't make a right, insofern heilt der Vergleich nicht das Problem der fehlenden Rechtssicherheit im Drittland USA.

Microsoft nach Schrems II

Nach Veröffentlichung der Begründung des EuGH-Entscheids hat Microsoft zügig die Online Service Terms (OST) sowie das zu diesem Zeitpunkt aktuell gültige Data Protection Addendum (DPA) angepasst und bspw. für eine Übermittlung von personenbezogenen Daten von Europa in ein Drittland ausnahmslos auf die Standarddatenschutzklauseln abgestellt. Um den vorgenannten Zusicherungen gerecht zu werden, wurden von Microsoft die OST und das DPA im September 2021[104] erneut angepasst bzw. entsprechende Neuerungen aufgenommen:

- Verschlüsselung bei Übertragung von Daten und bei data-at-rest
- Anspruch auf Schadensersatz bei unrechtmäßiger Verarbeitung von Daten
- Informationspflicht, wenn Microsoft durch staatliche Anordnung verpflichtet wurde, Daten an US-Sicherheitsbehörden herauszugeben
- Verpflichtung den Rechtsweg zu beschreiten und US-Gerichte anzurufen, um behördliche Anordnungen zur Herausgabe der Daten anzufechten

Damit verpflichtet sich Microsoft, Daten von Unternehmenskunden und Kunden aus dem öffentlichen Sektor zu schützen und sie keiner unangemessenen Offenlegung auszusetzen. Diese Schutzmaßnahmen nennt Microsoft „Defending Your Data"[105] und hat sie als Anhang C in das DPA aufgenommen. Microsoft prüft fortlaufend, ob und welche weiteren ergänzenden Maßnahmen angemessen sind, um den Anforderungen des Europäischen Datenschutzausschusses ausreichend Rechnung zu tragen.

Damit Bestandskunden von dieser Regelung ebenfalls profitieren und die Änderungen rechtswirksam in ein bestehendes Vertragsverhältnis aufgenommen werden, können bspw. Enterprise Agreement-Kunden seit Januar 2021 über ihren Distributor einen entsprechenden Vertragszusatz (Amendment) anfordern. Ausführliche Fragen und Antworten zur aktuellen Entwicklung hat Microsoft im Dezember 2021 im „Microsoft Cloud Compendium" zusammengefasst.[106]

[102] Law Enforcement Requests Report, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report, Abruf am 08.04.2022.
[103] https://www.microsoft.com/de-de/download/details.aspx?id=50830, zuletzt abgerufen am 12.09.2022
[104] Additional Safeguards Addendum to Standard Contractual Clauses, https://news.microsoft.com/wp-content/uploads/prod/sites/442/2021/01/REFERENCE-COPY-Additional-Safeguards-Addendum-to-Standard-Contractual-Clauses-.pdf, Abruf am 08.04.2022.
[105] https://news.microsoft.com/de-de/neue-massnahmen-zum-schutz-von-daten, zuletzt abgerufen am 12.09.2022
[106] https://www.microsoft.com/de-de/download/details.aspx?id=50830, Abruf am 08.04.2022.

Allerdings stehen die Neuregelungen in der Kritik: So wird etwa moniert, dass die Klauseln an keiner Stelle eine Information der betroffenen Personen vorsehen, wenn Microsoft ihre personenbezogenen Daten an Behörden von Drittländern herausgibt. Ohnehin wird man vor dem tatsächlichen Problem stehen, dass ggf. aufgrund der nationalen Gesetzgebung des Drittlandes ein Informieren des Betroffenen gesetzlich untersagt ist.[107]

Eine vertraglich zugesicherte Informationspflicht besteht für Microsoft insofern nur gegenüber ihren (Vertrags-)Kunden. Und auch der Anspruch auf Schadensersatz sei faktisch ausgeschlossen, da die Bedingungen für die Durchsetzung des vertraglichen Anspruchs praktisch nicht erfüllbar sind und von vornherein alle grundrechtlich unzulässigen Zugriffe von US-Behörden von der Regelung ausgenommen sind.

Das niederländische Ministerium für Justiz und Sicherheit hat im Februar 2022 eine DSFA in Bezug auf Microsoft Teams, OneDrive, SharePoint und Azure AD veröffentlicht, welche die Risiken jedoch gemäßigter beurteilt als in der Vergangenheit.[108]

Update – Anpassung des DPA:

Im September 2022 hat Microsoft sein DPA erneut angepasst und veröffentlicht. Im DPA wurden die EU-Standarddatenschutzklauseln von 2010 entfernt. Grund hierfür ist, dass zum einen die EU-Standarddatenschutzklauseln von 2010 spätestens bis Dezember 2022 durch die EU-Standarddatenschutzklauseln von 2021 ersetzt werden müssen. Zum anderen ist Microsoft Irland seit 2021 alleiniger Vertragspartner für EU-Kunden. Das bedeutet, dass die Übermittlung von personenbezogenen Daten auf Grundlage von EU-Standarddatenschutzklauseln zwischen Microsoft Irland und dem Mutterkonzern vereinbart werden (Modul 3: Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter) müssen. EU-Kunden und Microsoft Irland schließen folglich nur (noch) einen Vertrag zur Auftragsverarbeitung. Gleiches gilt für die Pflicht zur Durchführung einer Transfer-Folgenabschätzung (TIA), die sich aus den EU-Standarddatenschutzklauseln von 2021 ergeben. Da Microsoft Irland als Datenexporteur agiert, liegt die Pflicht zur Erstellung bei eben dieser Stelle. Dieser Pflicht ist Microsoft bereits nachgekommen und hat die TIA veröffentlicht.

Update – Einschätzung der Datenschutzkonferenz zu Microsoft-Onlinediensten:

Am 24.11.2022 hat die Datenschutzkonferenz entschieden, dass „der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden kann.“ Darüber hinaus heißt es, dass „solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.“[109] Die Einschätzung der DSK zum datenschutzkonformen Einsatz von Microsoft ändert sich somit vorerst nicht. Die Datenschutzbehörden beurteilen den Einsatz weiterhin kritisch. Microsoft hat sich zu der Einschätzung der DSK geäußert und teilt die Position der DSK (erwartungsgemäß) nicht. Microsoft stelle sicher, dass die M365-Produkte die strengen EU-Datenschutzgesetze nicht nur erfüllen, sondern oft sogar überträfen. Microsoft-Kunden in Deutschland und der gesamten EU können, nach Meinung von Microsoft, die M365-Produkte weiterhin bedenkenlos und rechtssicher nutzen.[110]

[107] Hansen-Oest: Drittlandsverarbeitung in Zeiten von Schrems II, in DSB 12/2020, S. 300 (S. 302)
[108] DPIA on Microsoft Teams, OneDrive SharePoint and Azure AD (June 2021), https://open.overheid.nl/repository/ronl-06f045ed745d9540ec4262a6079e8e73ad262a43/1/pdf/Public%20DPIA%20Teams%20OneDrive%20SharePoint%20and%20Azure%20AD%2016%20Feb%202022.pdf, Abruf am 09.01.2023.
[109] https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf, Abruf am 05.12.2022
[110] https://news.microsoft.com/de-de/microsoft-erfuellt-und-uebertrifft-europaeische-datenschutzgesetze/, Abruf am 05.12.2022

Ausblick: Trans-Atlantic Data Privacy Framework

Im März 2022 haben die Europäische Kommission und die USA eine grundsätzliche Einigung über einen transatlantischen Rahmen (Framework) für den Datenschutz verkündet.[111] Die Ankündigung beruht auf fünf wichtigen Grundsätzen (Key Principles):

- Auf Grundlage des neuen Frameworks soll der freie und sichere Datenverkehr zwischen der EU und teilnehmende US-Unternehmen möglich gemacht werden.
- Ein neues Regelwerk und verbindliche Garantien sollen den Zugriff auf Daten durch US-Geheim- bzw. Nachrichtendienste („zum Schutz der nationalen Sicherheit“) auf ein notwendiges und verhältnismäßige Maß beschränken; die Nachrichtendienste sollen Verfahren einführen, die eine wirksame Überwachung der (neuen) Datenschutz- und Grundrechte sicherstellen.
- Ein neues zweistufiges Rechtsbehelfssystem zur Untersuchung und Beilegung von Beschwerden der Europäer über den Zugang zu Daten durch US-Geheimdienste, einschließlich eines Datenschutzüberprüfungsgerichts, soll entstehen.
- Es soll strenge Verpflichtungen für Unternehmen geben, die aus der EU übermittelte Daten verarbeiten. Die Einhaltung der Grundsätze und Verpflichtungen soll mittels eine Selbstzertifizierung beim US-Handelsministerium realisiert werden.
- Spezifische Überwachungs- und Überprüfungsmechanismen sollen entstehen.

Aus Sicht der Verhandlungsparteien ergeben sich aus einem neuen Abkommen folgende Vorteile:

- Angemessener Schutz der in die USA übermittelten Daten von Europäern unter Berücksichtigung des Urteils des EuGH (Schrems II)
- Sicherer und geschützter Datenverkehr
- Dauerhafte und zuverlässige Rechtsgrundlage
- Wettbewerbsfähige digitale Wirtschaft und wirtschaftliche Zusammenarbeit
- Kontinuierliche Datenströme, die den grenzüberschreitenden Handel in Höhe von 900 Mrd. EUR pro Jahr unterstützen

Hierbei handelt es sich jedoch bislang nur um eine grundsätzliche Einigung. Die Parteien haben angekündigt, die Verhandlungsergebnisse in rechtliche Dokumente zu übersetzen. Auch wenn Microsoft sich optimistisch zeigt,[112] bleibt es fraglich, ob es noch im Jahr 2022 zu einem Nachfolger des EU-US-Privacy Shields kommen wird und ob dieses Nachfolgeabkommen auf stabileren Beinen stehen wird als seine Vorgänger.

Update – Executive Order:

US-Präsident Joe Biden hat im Oktober 2022 die „Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities” unterzeichnet.[113] Auch wenn die Executive Order keine direkte Wirkung auf die EU hat, macht sie dennoch den Weg für die Prüfung eines neuen Angemessenheitsbeschluss der EU-Kommission für einen Datentransfer in die USA frei. Landesdatenschützer wie Dr. Brink

[111] Siehe https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf, zuletzt abgerufen am 31.03.2022
[112] EU-U.S. data agreement an important milestone for data protection, Microsoft is committed to doing our part, https://blogs.microsoft.com/eupolicy/2022/03/25/eu-us-data-agreement-an-important-milestone-for-data-protection-microsoft-is-committed-to-doing-our-part, Abruf am 07.04.2022.
[113] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/, Abgerufen am 05.12.2022

(Baden-Württemberg) begrüßen zwar die Executive Order und erkennen diese ebenfalls als wichtigen Schritt an, äußern jedoch gleichzeitig Kritik und stellen erhebliche rechtliche Unklarheiten heraus.[114]

[114] https://www.baden-wuerttemberg.datenschutz.de/usa-eu-datentransfer-durchfuehrungsverordnung-us-praesident/ , Abgerufen am 05.12.2022

VI. Mitarbeitervertretung/Personal- bzw. Betriebsrat als Wegbegleiter und weitere Stakeholder

Kann M365 einfach in Organisationen eingesetzt werden? Müssen Betriebsrat bzw. Mitarbeitervertretung mitbestimmen?

Betriebs-/Personalrat bzw. Mitarbeitervertretung sind vom Arbeit- resp. Dienstgeber rechtzeitig vor Einführung von M365 mit ins Boot zu holen. Sie stehen dabei vor den folgenden Herausforderungen:

- *SaaS-Modelle unterliegen einer steten Veränderung,*
- *Self-Service-Auswertungen via Apps sind tägliche Realität.*
- *die Auswirkungen auf Datenschutz sowie Verhaltens- und Leistungskontrolle ändern sich fortlaufend.*
- *die Verweigerung der Datenverarbeitung gefährdet i. d. R. den Geschäftserfolg des Unternehmens.*

Die Verwendung von M365 berührt zahlreiche Beteiligungsrechte, insbesondere eine Mitbestimmung bzgl. der Einführung und Anwendung von technischen Einrichtungen. Vor der Einführung ist daher zwingend der Betriebsrat (BR), der Personalrat (PR) bzw. die Mitarbeitervertretung (MAV) in den Beschaffungsvorgang einzubinden. Applikationen wie Microsoft Teams oder Forms bedürfen der Zustimmung durch die Interessenvertretungen der Arbeitnehmerinnen und Arbeitnehmer (BR/PR/MAV), da es sich hier um die Einführung und Anwendung technischer Einrichtungen handelt, die die Möglichkeit eröffnen, das Verhalten oder die Leistung der Mitarbeiterinnen und Mitarbeiter zu überwachen.[115]

Darüber hinaus benötigt der Arbeit- bzw. Dienstgeber für die Verarbeitung von Mitarbeiterdaten, die nicht zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich werden, eine Rechtsgrundlage. Diese kann sich aus dem Datenschutzrecht selbst oder einer anderen Rechtsvorschrift ergeben. Wie im Kontext der Videokonferenzen[116] besteht die Möglichkeit, mit der Mitarbeitervertretung eine Kollektivvereinbarung (in Ausgestaltung einer Betriebs- oder Dienstvereinbarung) zu schließen.

Grundsätzlich müssen sich die Interessenvertreter häufig bei der Nutzung von M365 mit folgenden Fragestellungen beschäftigen:

Auftragsverarbeitung von Mitarbeiterdaten (siehe Kapitel IV) – Rollen- und Rechtekonzept.

Fortlaufende Veränderung der Software (SaaS) –Mandantentrennung

Informationssicherheit – Verschlüsselung und Maßnahmen nach dem Stand der Technik

Datenschutz & Compliance – Erfüllung der datenschutzrechtlichen Anforderungen und aller gesetzlichen und vertraglichen Regelungen

Accountability & Transparenz – Umgang, Nachweisbarkeit (Dokumentation) und Rechenschaft bzgl. Verhaltens- und Leistungskontrollen und bzgl. Fragen der Ordnung und des Verhaltens im Betrieb

Problematisch dürfte vielfach sein, ob die Mitarbeitervertretung angesichts der immer wieder in Diskussion stehenden datenschutzrechtlichen Bedenken gegenüber Microsoft-Produkten und den Potentialen bzgl. Mitarbeiterüberwachung, die diese technische Einrichtung bietet, generell zustimmen mag. Zudem erleichtern die stetig steigende Komplexität der Systeme und die damit einhergehende Intransparenz eine Entscheidung nicht.

[115] Siehe bspw.§ 36 Abs. 1 Nr. 9 MAVO
[116] Siehe Frage 0

Zumindest in Bezug auf datenschutzrechtliche Belange hat eine Mitarbeitervertretung jedenfalls kein unmittelbares Mitbestimmungsrecht. Allerdings kommt der Mitarbeitervertretung eine Überwachungsfunktion dergestalt zu, dass zugunsten der Arbeitnehmer geltende Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen zur Anwendung kommen und eingehalten werden. Um dieser Aufgabe gerecht zu werden, haben Arbeitnehmervertretungen Anspruch auf umfangreiche Informationen gegenüber dem Arbeit- bzw. Dienstgeber. Durch diese kann letztlich der Arbeitnehmerdatenschutz gewährleistet werden.

So können etwa bei der Auftragsverarbeitung Mitarbeiter des Dienstleisters grundsätzlich oder anlassbezogen Zugriff auf die (Mitarbeiter-)Daten der Organisation erhalten. Es braucht damit – nicht nur für den internen Zugriff – zwingend ein Rollen- und Berechtigungskonzept. Während beim Outsourcing bzw. Hosting in der Regel eine kundenspezifische Infrastruktur aufgebaut und betrieben wird, nutzen bei SaaS-Modellen mehrere Kunden dieselbe Infrastruktur. Mandantentrennung muss also das oberste Gebot sein.

In Summe sollten Dienstgeber und Arbeitnehmervertreter daher für die Einführung von M365 eine Betriebs- oder Dienstvereinbarung schließen, die mindestens folgende Punkte regelt:

- Geltungsbereich (sachlich, persönlich)
- Funktionsumfang
- (Beschäftigten-)Datenschutz, Daten- und Informationssicherheit
- Rollen- und Berechtigungskonzept
- Protokollierung
- Schnittstellen
- Löschung der Benutzerkonten und Löschfristen
- Verzicht auf Verhaltens- und Leistungskontrolle
- Anlage der zugelassenen Dienste/Applikationen

Aufgrund der Entwicklungsdynamik und der z. T. umfassenden Möglichkeiten zur Verhaltens- und Leistungskontrolle durch den Arbeitgeber empfiehlt es sich, eine Rahmendienstvereinbarung und für die Applikationen jeweils eine Dienstvereinbarung als Anlage zum Rahmenvertrag zu verhandeln. In der Rahmenvereinbarung sollte klarstellend festgehalten werden, dass die Microsoft-Produkte nicht oder nur in einem gemeinsam definierten Umfang zur Kontrolle der Mitarbeitenden herangezogen werden.

Zudem können die Parteien ein sogenanntes „Auto-Approval“ vereinbaren, sofern sie insbesondere die datenschutzrechtlichen Anforderungen erfüllt. Dies bedeutet, dass eine neue Anwendung ohne vorherige Prüfung durch die Mitarbeitervertretung als freigegeben betrachtet werden darf, sofern sie insbesondere den datenschutzrechtlichen Prüfungen standhält.

Datenschutz, Compliance und IT-Security

Gemäß den einschlägigen Datenschutzgesetzen im weltlichen und kirchlichen Bereich müssen Datenverantwortliche eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) für die Verarbeitung von Vorgängen vorbereiten, die „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach sich ziehen“. Ob eine Datenschutz-Folgenabschätzung erforderlich ist, hängt von den jeweiligen in M365 zu verarbeitenden Daten ab und davon, wie die Organisation als Datenverantwortlicher M365 bereitstellen, konfigurieren und verwenden möchte.

Es empfiehlt sich, sofern bestellt resp. vorhanden, den Datenschutzbeauftragten sowie die Fachbereiche/Abteilungen Compliance und IT-Security frühzeitig einzubinden. Die fachlichen Experten sollten sich sodann u. a. mit folgenden Punkten im Kontext des Unternehmens und der Einführung von M365 auseinandersetzen:

- Business Continuity
- Risikoeinschätzung und -bewertung
- Datenschutzfolgenabschätzung
- Datenklassifizierung

- Definition geeigneter Policies
- Definition technischer und organisatorischer Maßnahmen

Für den Prüfbereich Compliance ist der Anforderungskatalog Cloud Computing (C5)[117] des Bundesamtes für Sicherheit in der Informationstechnik eine wertvolle Orientierung. Mittels Anforderungskatalog lassen sich die u. a. die folgenden Kriterien eines Cloud Services auf Belastbarkeit und Vorhandensein hin überprüfen:

Organisation der Informationssicherheit	Identitäts- und Berechtigungsmanagement	Steuerung und Überwachung von Dienstleistern und Lieferanten
Sicherheitsrichtlinien und Arbeitsanweisungen	Kryptografie und Schlüsselmanagement	Security Incident Management
Personal und Verantwortlichkeiten	Kommunikationssicherheit	Sicherstellen des Geschäftsbetriebs und Notfallmanagement
Asset Management	Portabilität und Interoperabilität	Sicherheitsüberprüfung und -nachweis
Physische Sicherheit	Beschaffung, Entwicklung und Änderung von Informationssystemen	Compliance und Datenschutz
Regelbetrieb, Datensicherung, Kapazitätsmanagement, Protokollierung		Mobile Device Management

Nach eigenen Angaben wurde für Microsoft Azure und Azure Government in mehr als 100 internationalen Microsoft-Rechenzentren, die durch unabhängige Prüfer von Deloitte vorgenommen wurde, die Erfüllung der C5-Anforderungen festgestellt.[118]

Weitere Stakeholder

Neben den bereits genannten Interessenvertretern sollte der am stärksten von der Einführung betroffene Personenkreis nicht aus dem Blickfeld geraten: die Mitarbeitenden. Die Organisation bzw. deren Mitarbeitenden sind eine lernende Einheit, für die es häufig mehr geben muss als reine Produktschulungen. Mit M365 stehen Werkzeuge und Dienste zur Verfügung, die einen Einfluss auf Arbeitsabläufe und die Zusammenarbeit haben. Viele Organisationen beschäftigen sich daher tiefergehend in diesem Zusammenhang mit Fragen zur Digitalisierung.

Um die Akzeptanz, Durchdringung und letztlich den Erfolg von M365 in der Organisation zu gewährleisten, müssen die Mitarbeitenden durch entsprechendes Kollaborations- und Schulungsangebote im Zuge der Einführung von M365 sinnvoll eingebunden werden.

[117] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 12.09.2022
[118] Siehe https://news.microsoft.com/de-de/microsoft-erfuellt-den-anforderungskatalog-cloud-computing-c5-des-bsi-fuer-mehr-als-100-seiner-weltweiten-rechenzentren/ (letzter Zugriff am 12.09.2022)

VII. Exit Management & Microsoft 365

Kommen wir da wieder raus? Zu Exit-Strategien bei Cloud-Diensten

Mit der Nutzung von Cloud-Lösungen begeben sich Organisationen in große Abhängigkeit. Nach Möglichkeit sollte mit Microsoft vor Vertragsschluss über eine Exit-Strategie verhandelt werden und entsprechende Regelungen fest vertraglich vereinbart sein.

Viele Normen wie z. B. die ISO 27001:2013 fordern von Unternehmen eine Strategie bzgl. Wechsel des oder Ausstiegs vom Cloud-Diensteanbieter. Eine Möglichkeit, um einen schnellen Anbieterwechsel vollziehen zu können, wäre der Aufbau einer (Multi-)Cloud-Management-Architektur. Gespeicherte Daten könnten so nahezu störungsfrei und ohne aufwändiges Migrationsprojekt von einem Cloud-Anbieter zum nächsten übermittelt werden. Soweit die Theorie, welche bei der Nutzung von CRM und ERP bereits an ihre praktischen und datenschutzrechtlichen Grenzen stößt.

Während für die Nutzung von Speicherlösungen oder auf Ebene des Host-Systems ein Wechsel von einer Cloud in die nächste noch vergleichsweise einfach erscheint, ist dies bei Einsatz einer Software-as-a-Service-Lösung (SaaS) ungleich schwieriger. Die neue Lösung müsste die gleichen Features bieten und vergleichbare Datenstrukturen abbilden, um eine nahtlose Datenübertragung zu ermöglichen. Es gibt auch andere Cloud-basierte Office-Suiten. Diese sind deutlich weniger verbreitet und nicht so akzeptiert wie die Lösungen von Microsoft. Daher ist es zweifelhaft, ob diese Alternativen sowohl den gleichen Funktionsumfang als auch einen höheren Datenschutz bieten. Zudem müssen die Alternativen mit den Office-Formaten kompatibel sein, da diese weiterhin die verbreitetsten Formate darstellen. Allein aus Kostengründen sollte eine Umstellung auf andere Systeme wohl überlegt sein.

Gleichwohl sollten mit Microsoft bestenfalls Vereinbarungen zur störungsfreien Überführung auf einen neuen Anbieter vereinbart werden. Microsoft selbst empfiehlt etwa die Erstellung eines grundsatzbasierten Dokumentes[119]. In Deutschland gibt es hierzu beispielsweise einen Orientierungsrahmen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)[120] im Kontext Clouddienste. Eine detaillierte Arbeitshilfe von Microsoft wird im Anhang erwähnt.

Allerdings darf man nicht vergessen, dass die Dienste von Microsoft als Massengeschäft ausgelegt sind, was der Aushandlung einer individuellen Vereinbarung entgegenstehen dürfte. Microsoft arbeitet in solchen Fällen mit einseitig vorformulierten Vertragszusätzen, die bei einigen Lizenzmodellen auf Anfrage ergänzend in das Vertragsverhältnis einbezogen werden können. Zur Regelung des „Exit Management" gibt es, Stand heute, allerdings seitens Microsofts keinen vertraglichen Zusatz, auf welchem man zurückgreifen könnte.

In den Bestimmungen für Onlinedienste (OST) oder Referenzdokumenten von Microsoft selbst ist ein Ausstieg nur kurz bzgl. Kündigungen behandelt, ausführliche Regelungen zum Exit fehlen:

> *„Durch Ablauf oder Kündigung des Onlinedienste-Abonnements des Kunden ändert sich nichts an der Pflicht des Kunden, für das Hosten seiner Kundendaten während einer Laufzeitverlängerung zu bezahlen*[121]*. (OST, Stand Februar 2021.)*

[119] https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=86271bef-0c15-4e1d-b429-e9a21a0a4f7f&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913, Auswahl „Compliance Guides", zuletzt abgerufen am 12.09.2022

[120] https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/BA/dl_181108_orientierungshilfe_zu_auslagerungen_an_cloud_anbieter_ba.pdf?__blob=publicationFile&v=4 (Zugriff am 12.09.2022)

[121] https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Zugriff am 12.09.2022)

Wenn Sie Ihr Abonnement vor Ende des Bereitstellungszeitraums kündigen, wird der Status „Abgelaufen" übersprungen, und es beginnt sofort der Status „Deaktiviert", der bei den meisten Abonnements, in den meisten Ländern und Regionen, 90 Tage dauert. Es empfiehlt sich, dass Sie vor der Kündigung Ihre Daten sichern. Allerdings können Sie als Administrator während des Status „Deaktiviert" weiterhin auf die Daten Ihrer Organisation zugreifen und sie sichern. Alle Kundendaten, die Sie zurücklassen, werden möglicherweise nach 90 Tagen, spätestens aber 180 Tage nach der Kündigung gelöscht. "[122]

Der Zeitraum 90 Tage ist im Übrigen auch im kirchlichen Bereich eine bekannte Größe, wo der Wechsel des (Cloud-)Anbieters innerhalb eines Zeitfensters von 90 Tagen erfolgen sollte – was bei den heute üblicherweise verarbeiteten Datenmengen eine enorme Herausforderung darstellen dürfte. So führt etwa das Katholische Datenschutzzentrum Frankfurt/Main aus, dass bei erzwungenen Vertragsbeendigungen eine realistische Exit-Strategie vorzuhalten ist, die es erlaubt, die an Microsoft ausgelagerten Dienste innerhalb der meistens 90-tägigen Kündigungsfrist ins eigene Haus oder zu anderen, datenschutzkonform arbeitenden Dienstleistern zu übertragen.[123]

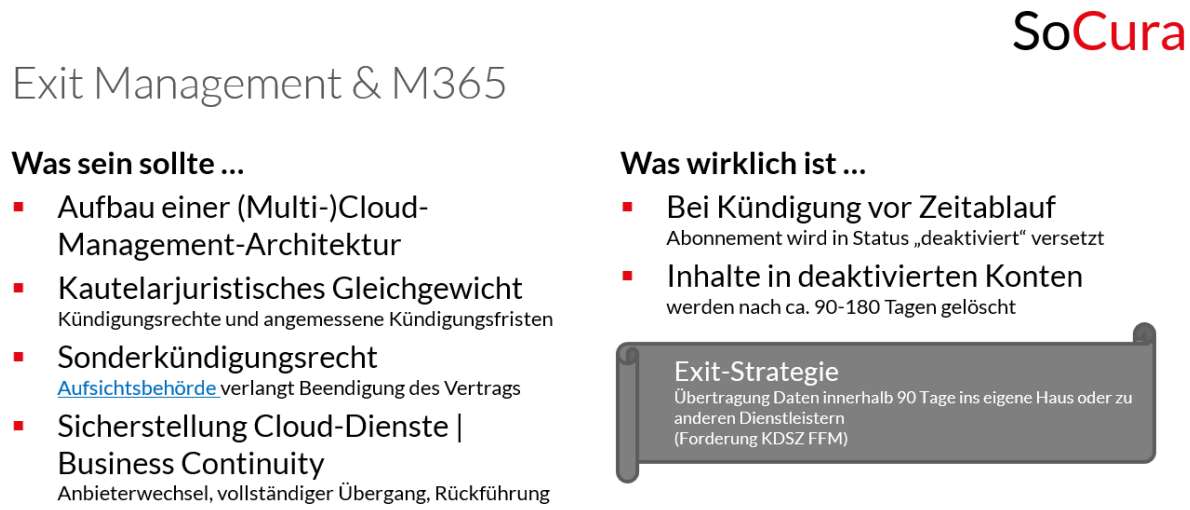


Abbildung 4: Exit Management & M365 – Wunsch und Wirklichkeit

Durch die Nutzung von M365 begibt sich die Organisation bekanntermaßen in eine gewisse Abhängigkeit, die im Falle von Microsoft als „Vendor-Lock-in" bezeichnet werden kann.[124] Dabei macht sich die Organisation von einem Anbieter derart abhängig, dass ein Wechsel zu einem anderen Anbieter nicht oder nur verbunden mit hohen Wechselkosten möglich ist.

Im Rahmen der Exit-Strategie muss daher geregelt sein, wie und wann die Daten herauszugeben sind. Zudem sollte Microsoft im Anschluss verpflichtet werden, alle eingebrachten und erzeugten Daten nachweislich und unwiederbringlich zu löschen. Zu fordern oder vielmehr zu wünschen wäre eine standardisierte Vereinbarung mit Microsoft zwecks Beauftragung von Unterstützungsleistungen (gegen Entgelt) auch nach Vertragsbeendigung bei Microsoft, um einen reibungslosen Wechsel oder eine Rückführung zu gewährleisten.

[122] https://docs.microsoft.com/de-de/microsoft-365/commerce/subscriptions/what-if-my-subscription-expires?view=o365-worldwide, Zugriff am 14.07.2022)
[123] Vgl. KDSZ-FFM: „Datenschutzrechtliche Bewertung eines Einsatzes von Office 365 auf der Plattform der Microsoft Cloud", https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/MS-Cloud-2019-KDSZ-FFM.pdf, zuletzt aufgerufen am 30.01.2021
[124] Weiterführend, auch zum Abhängigkeitsrisiko in Bezug auf die vom Anwender in das System eingegebenen und dort erzeugten Daten siehe Roth-Neuschild: Cloud Way out, ITRB 2013/9, S. 213 (S. 215)

Zusammenfassung und Fazit

Die Fragen rund um die die Einführung und den Lebenszyklus von M365 sind vielfältig und nicht nur aufgrund der technischen Entwicklungen und der Veränderungen in der Arbeitswelt dynamisch. Allein die Auswirkungen und Neuerungen im Kontext Schrems II haben bei der Entstehung der Orientierungshilfe wiederholt für Anpassungsbedarf gesorgt. Die grundsätzlichen Fragestellungen und zu betrachtenden Risiken bei Einführung und Nutzung von M365 bleiben dabei jedoch erhalten: Es ändert sich nur ab und an die Blickrichtung.

Während der rechtliche Rahmen noch viele Unsicherheiten birgt, hat sich Microsoft 365 in Zeiten von Pandemie und Homeoffice stark verbreitet. Nach Wahrnehmung der Autoren setzen viele Organisationen die Cloud-Dienste von Microsoft ein.

Die Einführung von M365 berührt zahlreiche datenschutzrechtliche Fragestellungen. An einigen Vorschriften in DSG-EKD und KDG (bzw. KDR-OG) bestehen – z. B. angesichts unzureichender Vorschriften in Bezug auf die Auftragsverarbeitung und des Drittlandtransfers – bis zur Klarstellung von gesetzgeberischer oder gerichtlicher Seite Zweifel an deren Europarechts-Konformität.[125]

Doch auch Microsoft hat weiterhin Grund zur Nachbesserung und weiteren Aufklärungen gegenüber Kunden und der Öffentlichkeit, etwa in Hinblick auf die gemeinsame Verantwortlichkeit.[126] So könnte man in Frage stellen, ob die Verarbeitung von Daten zu eigenen Zwecken für Microsoft bzgl. deren Verwertung am Ende des Tages nicht doch eine eigene resp. eine gemeinsame Verantwortlichkeit begründet.[127]

Insofern kann an dieser Stelle jedenfalls das „Versprechen“ aus der Einleitung gehalten werden: Die Auseinandersetzung mit der Orientierungshilfe schafft keine klare Antwort auf die Frage, ob der Einsatz von M365 rechtlich wie technisch bedenkenlos möglich ist. Sie hilft aber hoffentlich dabei, sich einen ersten Überblick über die Risiken und Chancen bei der Entscheidung für eine Einführung von M365 zu verschaffen. Eine tiefergehende Betrachtung kann jedoch stets nur im konkreten Einzelfall und im Kontext der eigenen Organisation erfolgen.

Um Ihnen dennoch eine kleine Hilfestellung mit auf den Weg zu geben, finden Sie nachfolgend die wichtigsten Fragestellungen in Form einer Checkliste zusammengefasst.

[125] Siehe ausführlich Golland: Reformation 2.0 – Umsetzung der Anforderungen der Datenschutz-Grundverordnung durch die evangelische und die katholische Kirche, RDV 2018, S. 8 (S. 13)
[126] Zur generellen Problematik siehe BGH, Urteil vom 05.06.2018 – Az. C-210/16
[127] Siehe exemplarisch Bericht der Berliner Aufsichtsbehörde: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf, zuletzt abgerufen am 12.09.2022

Checkliste vordringlicher Handlungsfelder

Lizenzmodelle & Pläne	Microsoft bietet eine Vielzahl von Abonnementverträgen und Volumenlizenzen (sogenannten Plänen). Im Bereich Kirche & Wohlfahrt haben Non-Profit-Organisationen die Möglichkeit via TSI-Programm[128] an den Lizenzprogramme Open Charity, Enterprise Agreement und CSP (Microsoft Volume Licensing - Optionen für Organisationen) teilzunehmen. In Hinblick auf die Lizenzierung sind der aktuelle Bedarf und die künftigen Anforderungen genau zu ermitteln. Die Produkte werden als Suiten zur Verfügung gestellt und reichen dabei von günstigen E1- F3 Lizenzen ohne lokal zu installierende Office-Anwendungen bis hin zu leistungsstarken E5-Lizenzen inkl. erweiterte Sicherheits-, Analyse- und Sprachfunktionen. Zusatzvereinbarungen, wie bspw. das erwähnte Amendment ID M657, können nach Absprache mit Microsoft im Rahmen eines Enterprise Agreements abgeschlossen werden.
Datenschutz, IT-Sicherheit & Compliance	Neben der Beachtung aktueller datenschutzrechtlicher Entwicklungen (bes. Schrems II) sollte bereits vor Einführung festgelegt werden, welche Daten mit welchen Applikationen innerhalb von M365 wie verarbeitet werden dürfen. Anhand der Festlegung ist sodann eine Subsumtion unter das vorhandene oder eine Implementierung in den Aufbau eines neuen Datenschutz- und IT-Sicherheitskonzept notwendig. Neben Beachtung der geltenden gesetzlichen Regelungen sind die vertraglichen und internen Vorgaben der Organisation in die Konzeption mit einzubeziehen. In vielen Fällen wir die Erstellung einer Risikoanalyse in Verbindung mit einer Datenschutz-Folgenabschätzung unumgänglich sein.
Mitbestimmung	Die Einführung von M365 berührt zahlreiche Beteiligungsrechte, insbesondere eine Mitbestimmung bzgl. der Einführung und Anwendung von technischen Einrichtungen. Die Mitarbeitervertretung ist **rechtzeitig vorab** einzubinden.
Laufendes Monitoring	Der Funktionsumfang von Microsoft 365 und anderen Cloud-Lösungen verändert sich laufend. Neue Features sind nicht immer nach dem „Privacy-by-Default“-Prinzip konzipiert. Es wird unerlässlich sein, die Aktualisierung und Erweiterung von Funktionen im Blick zu behalten und Konfigurationseinstellungen und laufend an aktuelle Begebenheiten anzupassen.
Exit Management	Viele Normen wie z. B. die ISO 27001:2013 fordern eine Strategie bzgl. Wechsel des oder Ausstiegs vom Cloud-Diensteanbieter. Die Entwicklung einer Exitstrategie ist keine einfache Aufgabe und sollte spätestens zum Zeitpunkt der Einführung von M365 vorhanden sein.

[128] Tech for Social Impact (TSI) ist ein Programm zur Rabattierung von Microsoft-Lizenzen für Non-Profit-Organisationen

Anhang

Autoren & Expertenkreis

ALTHAMMER & KILL

Digitalisierung sicher gestalten – an der Schnittstelle von Recht und Technik im Gesundheits- und Sozialwesen sowie anderen Branchen

Kontakt: info@althammer-kill.de

Simon Lang

General Management (M.A.), Produktmanager Althammer & Kill

Erfahrung in der Beratung als zertifizierter Datenschutzbeauftragter, heute verantwortlich für die Bereiche Produkte & Marketing.

Thomas Althammer

Wirtschaftsinformatiker, Geschäftsführer Althammer & Kill

Berät mit seinem 45-köpfigen Team Träger und Einrichtungen im Bundesgebiet zu den Themen Datenschutz, Informationssicherheit und IT-Compliance, z. B. mit der Erstellung von DSFA für Microsoft 365.

SoCura

Buchhaltungs-, IT- und Personal-Services für Wohlfahrtseinrichtungen als Service-Gesellschaft im Malteser-Orden

Kontakt: it-compliance@socura.de

Philip Huefnagels-Vajda

Wirtschaftsjurist und zertifizierter Mediator, Teamleiter Recht & Compliance bei der SoCura

Verantwortlich für IT-Vertragswesen und IT-Richtlinien im Verbund der Malteser

Dr. Karsten C. Ronnenberg

Datenschutzbeauftragter der Malteser, zertifizierter Datenschutzbeauftragter, Althistoriker

Berät in Fragen zu Datenschutz und IT-Compliance

Wir bedanken uns bei den folgenden Experten für Ihre Unterstützung als Kommentatoren der Erstausgabe und für den laufenden fachlichen Austausch:

Stefan Banning, Datenschutzbeauftragter (Köln)
Diözesan-Caritasverband (DiCV) für das Erzbistum Köln e. V.
Dachverband der kath. Wohlfahrtspflege im Erzbistum Köln

Henning Bergmann, Datenschutzbeauftragter (Köln)
SoCura Systems GmbH
Buchhaltungs-, IT- und Personal-Services für Wohlfahrt und Kirche

Alexander Gottwald, Rechtsanwalt & Datenschutzbeauftragter (Münster)
Solidaris Rechtsanwaltsgesellschaft mbH
Wirtschaftsprüfung, Steuer- und Rechtsberatung

Joerg Heidrich, Rechtsanwalt (Hannover)
Kanzlei Heidrich Rechtsanwälte
Fachanwälte für IT-Recht, Schwerpunkt Internet-/Datenschutzrecht

Gerhard Holzer, Leiter IT & Datenschutz-Koordinator (Köln)
Malteser Hilfsdienst gGmbH
Bundesweit tätige Hilfsorganisation

Ziar Kabir, Rechtsanwalt & Datenschutzbeauftragter (Bad Honnef)
SCO-CON:SULT GmbH
Externe Datenschutzbeauftragte im Umfeld Kirche, NGO und Industrie

Christian Krug, GF, und Patric Rudtke, DSB (Sennfeld)
VINTIN Services GmbH
IT-Systemhaus mit Schwerpunkt im Gesundheits- und Sozialwesen

Alexander Overmann, Datenschutzbeauftragter (Paderborn)
Connext Communication GmbH
Software-Anbieter in der Sozial- und Gesundheitswirtschaft

Mark Rüdlin, Rechtsanwalt & Datenschutzbeauftragter (Hamburg)
Rechtsanwaltskanzlei Mark Rüdlin
Schwerpunkt Datenschutz in medizinischen und sozialen Einrichtungen

Dr. Christoph Wegener, Informationssicherheitsexperte (Gevelsberg)
wecon.it-consulting
Beratung im Bereich Informationssicherheit und Datenschutz

Glossar & Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AO	Abgabenordnung
AV	Auftragsverarbeitung – früher Auftragsdatenverarbeitung (ADV)
BAGFW	Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege
BayKrG	Bayerisches Krankenhausgesetz
BDSG	Bundesdatenschutzgesetz
BfD EKD	Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland
BR	Betriebsrat
BYOK	Bring your own key – Modell der Verschlüsselung, in dem der Nutzer selbst den Schlüssel generiert
CLOUD Act	Clarifying Lawful Overseas Use of Data-Act – Gesetz, mit dem US-Behörden Zugriffe auf Daten von Kunden US-amerikanischer Firmen legitimieren
CRM	Customer-Relationship-Management
CSP	Cloud Solution Provider
data at rest	Daten, die gespeichert sind, ohne bewegt zu werden
data in transit	Daten, die zwischen verschiedenen Orten bewegt werden
DKE	Double Key Encryption
DPA	Data Protection Addendum – Vereinbarung zur Auftragsverarbeitung
DSG-EKD	Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments („Datenschutz-Grundverordnung“)
EBA	European Banking Authority
EDSA	Europäische Datenschutzausschuss, ehemals Artikel-29-Arbeitsgruppe (Brüssel)
ERM	Enterprise Resource Planning
EuGH	Europäischer Gerichtshof (Sitz: Luxemburg)
EU-US Privacy Shield	Datenschutz-Abkommen zwischen EU und USA, gekippt durch das EuGH-Urteil vom 16. Juli 2020 (Schrems II)
FIPS	Federal Information Processing Standard
FISA	Foreign Intelligence Surveillance Act (USA)
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
HYOK	Hold your own key – Modell der Verschlüsselung, in dem Microsoft den Schlüssel generiert, den der Nutzer jedoch aufbewahrt
IPSec	Internet Protocol Security
KDG	Gesetz über den Kirchlichen Datenschutz – Das Datenschutzgesetz der römisch-katholischen Kirche in Deutschland

KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz – Konkrete Vorgaben v.a. in Hinblick auf die Sicherheit der Verarbeitung
KDR-OG	Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts – Das Datenschutzgesetz der Deutsche Ordensobernkonferenz (DOK), weitgehend wortgleich mit dem KDG
KDR-OG-DVO	Durchführungsverordnung zur Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts – Konkrete Vorgaben v.a. in Hinblick auf die Sicherheit der Verarbeitung, stark angelehnt an die KDG-DVO
KDSZ	Katholisches Datenschutzzentrum (hier: Dortmund), das zusammen mit dem KDSZ in Frankfurt sowie drei weiteren Aufsichtsbehörden Mitglied der Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschlands ist
LAG	Landesarbeitsgericht
LfDI	Landesbauftragte(r) für Datenschutz und Informationssicherheit
M365	Microsoft 365 – Nachfolgeprodukt zu Office 365 (O365)
MAV	Mitarbeitervertretung
MfA	Multi-Faktor-Authentifizierung
MTLS	Mutual Transport Layer Security
MVLP	Microsoft Volumenlizenzprogramm
NSL	National Security Letters (USA)
OST	Online Service Terms
PR	Personalrat
S/MIME	Secure / Multipurpose Internet Mail Extensions – Standard für Verschlüsselung und Signierung
SaaS	Software as a Service – Software, die bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt wird.
Schrems II	Urteil des EuGH vom 16. Juli 2020 (Rechtssache C-311/18), mit dem das EU-US Privacy Shield unwirksam wurde, benannt nach dem Beschwerdeführer Max Schrems
SGB	Sozialgesetzbuch
SRTP	Secure Real-Time Transport Protocol
StGB	Strafgesetzbuch
TADPF	Trans-Atlantic Data Privacy Framework
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TSI	Tech for Social Impact – Programm zur Rabattierung von Microsoft-Lizenzen für Non-Profit-Organisationen
TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien
UWG	Gesetz gegen den unlauteren Wettbewerb

Weiterführende Literatur

Dieses Whitepaper verweist in den Fußnoten auf eine Vielzahl von Quellen und Informationen. Für eine weiterführende Auseinandersetzung mit den Themen möchten wir insbesondere auf die folgenden Seiten und Ressourcen hinweisen:

Microsoft Service Trust Portal https://servicetrust.microsoft.com/ https://docs.microsoft.com/de-DE/compliance/regulatory/offering-home	Überblick und Einsichtnahme in **Audit-Reports** zu Microsoft Cloud-Diensten, u. a. erhältlich auf Grundlage der ISO 27000-Familie., IT-Grundschutz und zu weiteren allgemeinen und branchenspezifischen Prüfungsstandards. Eine Datenbank erlaubt die Recherche nach einzelnen Berichten basierend auf unterschiedlichen Kriterien. Eine Übersichtsseite stellt die wichtigsten Compliance-Standards gruppiert nach Branche und Region tabellarisch dar.
Microsoft Transparenzberichte https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report	Im Bereich **Corporate Social Responsibility** finden sich bei Microsoft Statistiken zu Anfragen von Strafverfolgungsbehörden. Anhand von Land, Region und Zeitraum lässt sich so ermitteln, wie interessiert die Behörden einzelner Länder an den bei Microsoft gespeicherten Daten tatsächlich sind. Ein zusätzlicher Bericht weist die Anfragen im Rahmen des nordamerikanischen Foreign Intelligence Surveillance Act (FISA) und durch National Security Letters (NSL) aus.
Microsoft Priva https://docs.microsoft.com/de-de/privacy/priva/priva-overview	Anfang 2022 wurde **Microsoft Priva** freigegeben, das als Bestandteil von Microsoft 365 bei der Umsetzung von DSGVO-Vorgaben unterstützt. Mit Priva Privacy Risk Management steht ein Modul für die organisationsbezogene Sicht auf Daten und Richtlinien im Kontext Datenschutz bereit. Priva Subject Rights Requests bietet Automatisierungs- und Workflowtools für die effiziente Beantwortung von Betroffenenanfragen.
Gutachten von Stephen I. Vladeck vom 15.11.2021 zur Rechtslage in den USA https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/20220125_dsk_vladek.pdf	Im Auftrag der **Datenschutzkonferenz** wurde im Rahmen eines Rechtsgutachtens die Anwendbarkeit des **Foreign Intelligence Surveillance Act (FISA)** bewertet und in welchem Umfang europäische Unternehmen aber auch Bürgerinnen und Bürger davon betroffen sind, wenn US-amerikanische Dienste eingesetzt werden.

Application of the CLOUD Act to EU Entities https://english.ncsc.nl/publications/publications/2022/augustus/16/memo-cloud-act	Bemerkenswertes **Memorandum** der Anwaltskanzlei GreenbergTraurig LLP zur Anwendbarkeit des **CLOUD Acts** auf europäische Unternehmen, selbst wenn diese nicht oder nur mit Tochtergesellschaften in den USA aktiv sind. Dahinter verbirgt sich die Frage, ob man bei Wahl eines europäischen (Cloud-)Anbieters den Gefahren des CLOUD Acts entgehen kann. Erstellt im Auftrag des Niederländischen Ministeriums für Justiz und Sicherheit (NCSC)
Microsoft-Statement zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/08/Microsoft-Statement_Datenschutzkonformitaet-von-Microsoft-365-und-Microsoft-Teams.pdf	**Stellungnahme von Microsoft** zu der Darstellung, dass Microsoft 365 oder Microsoft Teams nicht datenschutzkonform eingesetzt werden können oder diese gar selbst nicht datenschutzkonform sind. Das Dokument versucht, einige Gerüchte bzw. unrichtige Aussagen richtigzustellen.
Mitbestimmung beim Einsatz von Cloud-Diensten https://sway.office.com/NnD7zky8kfVik0wG	Handreichung von Microsoft-Mitarbeitenden zu den Unterschieden zwischen traditioneller Software und **Clouddiensten** und wie in diesem Zusammenhang die **Mitbestimmung im Unternehmen** organisiert werden kann.
Exit Planning for Microsoft Cloud Services https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWBkvx	Umfangreiche Handreichung von Microsoft im Kontext von Finanzinstitutionen zur **Gestaltung der Exit-Strategie bei Einsatz von Clouddiensten**.

Liste der kirchlichen Datenschutzaufsichtsbehörden

Katholische Datenschutzzentren und -beauftragte

Katholisches Datenschutzzentrum Frankfurt/Main (https://www.kath-datenschutzzentrum-ffm.de/)	▪ Erzdiözese Freiburg ▪ Bistum Fulda ▪ Bistum Limburg ▪ Bistum Mainz ▪ Bistum Rottenburg-Stuttgart ▪ Bistum Speyer ▪ Bistum Trier
Katholisches Datenschutzzentrum Dortmund (https://www.katholisches-datenschutzzentrum.de/)	▪ Bistum Münster ▪ Bistum Paderborn ▪ Bistum Essen ▪ Bistum Aachen ▪ Erzbistum Köln
Katholische Datenschutzaufsicht Nord (https://www.kdsa-nord.de/der_ddsb)	▪ Erzbistum Hamburg ▪ Bistum Hildesheim ▪ Bistum Osnabrück ▪ Bischöflich Münstersche Offizialat in Vechta i.O.
Der Diözesandatenschutzbeauftragte für die bayerischen (Erz-)Diözesen (https://www.erzbistum-muenchen.de/ordinariat/datenschutzstelle)	▪ Bistum Würzburg ▪ Bistum Regensburg ▪ Bistum Passau ▪ Bistum Eichstatt ▪ Bistum Augsburg ▪ Erzbistum München | Freising ▪ Erzbistum Bamberg
Kirchliche Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs (https://www.kdsa-ost.de/)	▪ Bistum Magdeburg ▪ Bistum Erfurt ▪ Bistum Görlitz ▪ Bistum Dresden Meißen ▪ Erzbistum Berlin

Datenschutzaufsicht der Evangelischen Kirche und ihre Regionen

Der Beauftragte für den Datenschutz der EKD Hauptsitz (https://datenschutz.ekd.de/)	▪ Evangelische Kirche in Deutschland (EKD) ▪ Union Evangelischer Kirchen in der EKD (UEK) ▪ Vereinigte Evangelisch-Lutherische Kirche Deutschlands (VELKD) ▪ Herrnhuter Brüdergemeine ▪ Evangelisches Werk für Diakonie und Entwicklung e.V. (EWDE) ▪ Deutsches Nationalkomitee des Lutherischen Weltbundes (DNK/LWB) ▪ Reformierter Bund in Deutschland
Der Beauftragte für den Datenschutz der EKD Datenschutzregion Nord (https://datenschutz.ekd.de/datenschutzrecht/ds-nord/)	▪ Braunschweig ▪ Bremen ▪ Hannover ▪ Oldenburg ▪ Reformiert ▪ Schaumburg-Lippe ▪ Konföderation ▪ Diakonisches Werk Bremen e.V. ▪ Diakonisches Werk evangelischer Kirchen in Niedersachsen e.V. ▪ Diakonisches Werk der Ev.-Luth. Kirche in Oldenburg e.V.
Der Beauftragte für den Datenschutz der EKD Datenschutzregion Ost (https://datenschutz.ekd.de/datenschutzrecht/ds-ost/)	▪ Berlin-Brandenburg-schlesische Oberlausitz ▪ Mitteldeutschland ▪ Diakonisches Werk Berlin-Brandenburg-schlesische Oberlausitz e.V. ▪ Diakonisches Werk Hamburg – Landesverband der Inneren Mission e.V. ▪ Diakonisches Werk Mecklenburg-Vorpommern e.V. ▪ Diakonisches Werk Schleswig-Holstein – Landesverband der Inneren Mission e.V.
Der Beauftragte für den Datenschutz der EKD Datenschutzregion Süd (https://datenschutz.ekd.de/datenschutzrecht/ds-sued/)	▪ Baden ▪ Bayern ▪ Württemberg ▪ Diakonisches Werk der Evangelisch-Lutherischen Kirche in Bayern e.V. ▪ Diakonisches Werk der evangelischen Kirche in Württemberg e.V. ▪ Diakonisches Werk der Ev. Landeskirche in Baden e.V.

Der Beauftragte für den Datenschutz der EKD Datenschutzregion Mitte-West (https://datenschutz.ekd.de/datenschutzrecht/ds-mitte-west/)	▪ Hessen und Nassau ▪ Kurhessen-Waldeck ▪ Lippe ▪ Rheinland ▪ Westfalen ▪ Diakonisches Werk in Hessen und Nassau und Kurhessen-Waldeck e.V. – Diakonie Hessen ▪ Diakonisches Werk Rheinland-Westfalen-Lippe e.V. – Diakonie RWL ▪ Diakonisches Werk der Evangelischen Kirche der Pfalz
Der Datenschutzbeauftragte der Nordkirche (https://datenschutz.ekd.de/datenschutzrecht/nordkirche/)	▪ Evangelisch-Lutherische Kirche in Norddeutschland
Unabhängige Aufsichtsbehörde für den Datenschutz in Kirche und Diakonie (https://dsbkd.de/)	▪ Evangelisch-Lutherische Landeskirche Sachsens ▪ Evangelische Landeskirche Anhalts ▪ Diakonie Sachsen ▪ Diakonie Mitteldeutschland
Die Datenschutzbeauftragte der Evangelischen Kirche der Pfalz (Protestantische Landeskirche) (https://www.evkirchepfalz.de/)	