Datenschutzregeln:

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

(gem. Artikel 30 Abs. 1 DSGVO)

sowie Datenschutzfolgeabschätzung

(gem. Art. 35 Abs. 1 i. V. m. Abs. 3b DSGVO)

Diese Niederschrift bezieht sich ausschließlich auf die Nutzung von Microsoft Office 365 im Rahmen der Verwendung am Berufskolleg Kleve und ist als Ergänzung zu bestehenden Verarbeitungsverzeichnissen zu verstehen. Es ist von vornherein für den Einsatz von Office 365 für Mitarbeitende und Lernende formuliert.

Inhaltsverzeichnis

1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit	Microsoft Office365 – Exchange, SharePoint, Teams sowie Installation der Desktop- und Mobilanwendungen
Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO (Bezeichnung der Hochschule, Anschrift, E-Mail- Adresse und Telefonnummer)	Berufskolleg Kleve Felix-Roeloffs-Str. 7 47533 Kleve Tel. 02821/7444? info@berufskolleg-kleve.de
Falls zutreffend: Angaben zu weiteren gemeinsam für die Verarbeitung Verantwortlichen (jeweils Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)	Cancom GmbH Messerschmittstr. 20 89343 Scheppach Lediglich Verlängerung der Lizenzen im Rahmen des „Campus FWU 4.0“ Vertrages
Datum der Einführung	01.02.2018
Stand dieser Dokumentation	16.02.2022
Behördlicher Datenschutzbeauftragter (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)	Landesdatenschutzbeauftragte Bettina Gayk Postfach 20 04 44 40102 Düsseldorf
Datenschutzbeauftragter des Berufskolleg Kleve	Michael Duismann michael.duismann@berufskolleg-kleve.de

2. Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b DSGVO)

Zweck	IT-gestützte Zusammenarbeit der Mitarbeitenden und Lernenden des Berufskollegs mittels der Microsoft Office 365 Dienste Exchange Online, Sharepoint Online und der Lernplattform Teams. Unterstützung des Berufskollegs bei der Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben mit Hilfe von Microsoft Office 365 zur Umsetzung des Bildungs- und Erziehungsauftrags, bei der Abwicklung der internen Aufgaben und Abläufe. Verwaltungs-tätigkeiten, z. B. die Zeugniserstellung gehören nicht dazu. Diese werden im sog. Verwaltungsnetz abgewickelt, das nicht in Verbindung mit Microsoft Office 365 steht. Besonders sind dies: • E-Mailkommunikation mit Termin- und Ressourcenverwaltung, gemeinsame Kalender, Office 365 Gruppen • Bereitstellung und Austausch von Dokumenten • Projektverwaltung zur Organisation der schulischen Abläufe, Chatfunktion • Lernplattform Teams mit Notizbüchern, Bereitstellung von Unterrichtsmaterialien, Aufgaben mit Terminabgabe, Rückmeldungen • Nutzung der Desktopversion von Office und mobiler Apps

Name des eingesetzten Verfahrens	Microsoft Office 365[1]
Dienstbeschreibungen	Eine aktuelle und vollständige Dienstbeschreibung ist bei Microsoft dokumentiert[2]

3. Rechtsgrundlagen:

- Bestimmungen der Schulvorschriften NRW
- Art. 6 Abs. 1 S. 1 lit c und e DSGVO
- Art. 6 und 9 DSGVO
- Zuständige Aufsichtsbehörde

4. Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)

- Mitarbeitende: Lehrkräfte, Personal der Schulverwaltung, Mitarbeitende der Schulsozialarbeit, Hausmeister*innen
- Alle Lernenden, die welche das Berufskolleg besuchen oder besucht haben (letzteres zeitlich eingeschränkt)

5. Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)

Daten zu Mitarbeitenden	• Grunddaten (Name, Vorname, Anzeigename, Anmeldename) • Gruppenzugehörigkeiten in Teams, ggf. Besitzerstatus • Weitere Daten, je nach Nutzung, z. B. Beiträge im Team, Aufzeichnungen im Kursnotizbuch
Daten der Lernenden	• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion) • Klassenbezeichnung • Gruppenzugehörigkeiten in Teams • Weitere Daten, je nach Nutzung, z. B. Beiträge im Team, Aufzeichnungen im Kursnotizbuch
Daten aller Nutzer	• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion) • Berechtigungen • Log-Daten (Datum der letzten Passwortänderung, Datum der letzten Anmeldung, Größe und Zahl der gespeicherten Daten; Login-Standort (ungenau), z. B. Düsseldorf oder Duisburg) • Historisierung (Information über angelegte/geänderte/gelöschte Datensätze)

[1] http://aka.ms/Wkcowi
[2] https://technet.microsoft.com/enus/library/office-365-service-descriptions.aspx

Von den Nutzern erzeugte Inhalte und Einstellungen	• persönliche Einstellungen • Angaben in Nutzerprofil • gespeicherte Inhalte in E-Mail, Chats, Kalendereinträge, Kommentare, Datenbankeinträge • Weitere Faktoren zur Anmeldung mittels Multi-Faktor-Authentifizierung (Telefon oder private E-Mail oder App oder Fragen)
Besondere Kategorien personenbezogener Daten (Art. 9)	keine

6. Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)

	Empfänger	**Zweck**	**Daten**
Intern	Mitarbeitende, Lernende	Zusammenarbeit und IT- gestützter Unterricht	Eingeschränkte Lese- und/oder Schreibrechten in den Teams und Office 365 Gruppen, deren Mitglied sie sind und in den Dokumentenbibliotheken und öffentlichen Kalendern, die ihnen freigegeben wurden.
	Systembetreuer	Konfiguration, Überwachung und Sicherung des Betriebs, Support	Administrative Lese-, Schreib- und Löschrechte entsprechend den ihnen zugeteilten Rechten auf alle oder bestimmte Office 365 Dienste
Extern	Alle Empfänger von E-Mails	Kommunikation	Anzeigename, E-Mailadresse
	Ireland Operations Limited, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Irland	Dienstbereitstellung, Service und Support	von den Benutzern gespeicherte Daten: Die Speicherung erfolgt nur innerhalb der EU in nach ISO 27001, 27002, ISO/IEC 27018 zertifizierten Rechenzentren im Rahmen des AV Vertrags[3] (Anhang 1), der die EU-Standardvertragsklauseln enthält. In der Regel ist der Speicherort Deutschland (z. B. Teams, Exchange, Sharepoint usw.) nur in Ausnahmefällen (z. B. Forms) ein anderes EU-Land[4] Anmeldedaten: Speicherung in allen Microsoft-Anmeldeservern

[3] http://aka.ms/Wkcowi i. V. m.
[4] https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?geo=UnitedStates%23germany&view=o365-worldwide#germany

7. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)

Microsoft Ireland hat sich den EU-Standardvertragsklauseln unterworfen und beschreibt den Zugriff auf Kundendaten.[5]

Wenn ein neuer Dienst in Office 365 angeboten wird, werden die damit verbundenen Daten oft in den USA verarbeitet. Diese Dienste werden von der innehabenden Person der Stabsstelle „Digitale Kommunikation, Information und Unterrichtsgestaltung“ ausgeschaltet, die Lizenz wird nicht an Lernende ausgegeben.

8. Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)

Verlässt eine Mitarbeiter*in oder Lernende(r) die Schule, wird das persönliche Office 365 Konto inklusive aller gespeicherten Daten gelöscht. Die Nutzerdaten können noch 30 Tage nach der Löschung wiederhergestellt werden. Danach sind die Daten unwiderruflich gelöscht.

9. Technische und organisatorische Maßnahmen (Art. 32 Abs. 1 DSGVO)

Die technisch-organisatorischen Maßnahmen in den EU-Rechenzentren von Microsoft Irland sind durch die Zertifizierung und die Angaben in diesem Link https://www.microsoft.com/de-de/trust-center/privacy aufgeführt. Die verbleibenden Maßnahmen, die hier beschrieben wird, sind die Maßnahmen zur Sicherung des Internet-Zugangs zu den Microsoft Diensten in Office 365 und zur sicheren Speicherung von Zugangsdaten auf den Clients des Verantwortlichen.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Kontrolle des Zutritts/ Zugangs/Zugriffs	die Anmeldung an Office 365 erfolgt mit Hilfe einer sog. „Reinen Cloud-Identität“. Jede teilnehmende Person erhält mit der Nutzerkennung ein Erstpasswort, welches bei der Erstanmeldung verändert werden muss. Jede teilnehmende Person darf das Zugriffspasswort selbst über ein Self-Care-Center ändern.
	Trennungskontrolle	Administrativer Zugriff auf die Office 365 Instanz des Berufskolleg Kleve ist auf die von der Schule ernannten Stabsstelle für digitale Kommunikation, Information und Unterrichtsgestaltung, Digitalisierungsberatende für jede Abteilung und die für die IT-Infrastruktur beauftragte Person beschränkt. Es ist geplant, weitere Personen mit der Verwaltung von Passwörtern zu betrauen, um einen

[5] https://www.microsoft.com/de-de/trustcenter/privacy/data-management/data-access

		reibungslosen Unterrichtsablauf zu gewährleisten.
Integrität (Art. 32 Abs. 1 lit. b DS-GVO)	Weitergabekontrolle	Im Rahmen der Nutzung von Microsoft Online Diensten liegt die Umsetzung der Weitergabekontrolle bei Microsoft. Microsoft setzt im Rahmen der Onlinedienste bei der Datenübertragung über das Internet auf TLS Verschlüsselung (https Protokoll)[6].
	Eingabekontrolle	Die Konsistenz und Gültigkeit der Benutzerkonten in den Office 365 Instanzen ist durch die Anmeldung der Benutzer, die Sichtbarkeit der Benutzerkonten in den Adresslisten und Verzeichnissen gewährleistet.
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Verfügbarkeitskontrolle	Alle Benutzer-Anmeldedaten und Nutzerdaten liegen in den Microsoft EU-Rechenzentren (i. d. R. in Deutschland) und sind durch die spezifischen Sicherheitsmaßnahmen von Microsoft geschützt, insbesondere durch die Backup-Strategien von Microsoft (Datei-Versionierung, Spiegelung der virtuellen Instanzen).
	Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);	Dies ist serverseitig durch die mehrfache Spiegelung der virtuellen Instanzen in den Office 365 Instanzen gesichert (Microsoft Servicevertrag), Nutzerdaten in Office 365 können vom Nutzer selbst mit einem Klick auf den Stand eines früheren Zeitpunkts wiederhergestellt werden.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)	Datenschutz-Management	Die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird durch die Zertifizierung des Auftragnehmers gemäß Art. 42 DS-GVO gesichert.
	Incident-Response-Management	Falls ein illegitimer Zugriff auf eine Office 365 Instanz erfolgt, sind 2 Szenarien möglich: es werden zusätzliche Konten erstellt oder es werden Konten gelöscht. Gelöschte Konten und damit zusammenhängende Daten und E- Mails können in Office 365 teils durch den Nutzer selbst, und teils durch einen speziellen Papierkorb, auf den nur der Administrator Zugriff hat, wiederhergestellt werden. Zusätzliche Konten erscheinen in

[6] https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption?view=o365-worldwide

		den Adressbüchern und können kurzfristig gelöscht werden.
	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);	Die Mitarbeiter werden von den Systembetreuern auf die Möglichkeiten der Pseudonymisierung und sparsamen Speicherung personenbezogener Daten in Office 365 hingewiesen und dabei unterstützt. (z. B. Weigerung der Standortfreigabe bei der Nutzung der mobilen Teams-App)
	Auftragskontrolle	Die Office 365 Instanz gehört dem Auftraggeber, der allein Zugriff auf die Nutzdaten hat. Dritte (z. B. Rechenzentren) werden nicht zur Verwaltung der Nutzerdaten eingesetzt.

10. Datenschutzfolgeabschätzung

Die Datenschutzfolgeabschätzung ist gem. Art. 35 Abs. 1 i. V. m. Abs. 3 lit b DSGVO nur dann erforderlich, wenn die Datenerhebung ein hohes Risiko für die Rechte von Freiheiten natürlicher Personen darstellt. Das ist zwar bezüglich der Office Instanz des Berufskolleg Kleve nicht der Fall, trotzdem sollen die Maßnahmen erläutert werden, die zum Schutze von Lernenden und Mitarbeitenden ergriffen werden, um datenschutzrechtlichen Bedenken entgegenzutreten und die Sicherheit aller Beteiligten zu gewährleisten. Unter Bezugnahme auf die sechs Datenschutz-Grundregeln der DSGVO sollen diese Maßnahmen im Folgenden erläutert werden:

Die sechs Datenschutz-Grundregeln für die Verarbeitung personenbezogener Daten in der DSGVO:

1. Rechtmäßigkeit und Transparenz

Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn der Erlaubnistatbestand nach Art. 6 Abs. 1 lit. a DSGVO vorliegt. Demnach muss jede/r Nutzer/in seine Einwilligung zu der Verarbeitung der sie betreffenden Daten für einen oder mehrere bestimmte Zwecke geben. Die Abgabe der Einwilligung ist rechtmäßig, sofern die/der Nutzer/in das sechzehnte Lebensjahr vollendet hat. Wurde das sechzehnte Lebensjahr noch nicht vollendet, so ist die Verarbeitung nur durch die Einwilligung oder Zustimmung des Trägers der elterlichen Verantwortung rechtmäßig. Das Berufskolleg Kleve verschärft diese Regel und bindet gesetzliche Vertreter bei allen minderjährigen Schülerinnen/Schülern bei der Einwilligung ein.
Die Erhebung, Verarbeitung und Speicherung der personenbezogenen Daten dient dem Ziel, den beteiligten Personen des Systems ‚Schule' ausgewählte Programme der Office 365 Anwendung, für den Zeitraum von Ein- bis Austritt aus dem System, kostenlos zur Verfügung zu stellen. Dies dient dem Zweck die Schulorganisation für die Nutzer/innen sowie der Erleichterung der digitalen untereinander in der Schule. Darüber hinaus wird das Softwarepaket für unterrichtliche Zwecke genutzt, z. B. im Rahmen des Unterrichts auf Distanz während Pandemie-Schutzmaßnahmen.
Die dafür notwendigen Daten werden zunächst von der Schule erhoben. Im Anschluss daran erhält der IT-Dienstleister „Mr. Byte", über den die Schule Office 365 bezieht, die

Daten, welcher dann die Einrichtung der jeweiligen Accounts vornimmt. Diese sowie weitere Daten, die bei der Benutzung verschiedener Office-Anwendungen anfallen, werden für den o. a. Zeitraum von der Microsoft Corporation in Deutschland (Teams, OneDrive, OneNote, Exchange) oder in anderen Mitgliedsstaaten der EU gespeichert .[7] Sie unterliegen somit der DSGVO einschließlich der ISO 27001 und der ISO 27018.[8] Die gespeicherten Daten werden anonymisiert (Einstellung durch die Administration der Schule gewährleistet), sodass sie keinem/keiner Nutzer/in zugeordnet werden kann.

2. Zweckbindung

Die personenbezogenen Daten dürfen nur für „festgelegte, eindeutige und legitime Zwecke“ verarbeitet werden.[4] Da alle Beteiligten des Systems Schule eine Office 365 Lizenz mit individueller Benutzerkennung erhalten, ist es erforderlich den Vor- und Nachnamen zu verarbeiten. Zudem ist es bei den Schülern/innen notwendig, die Klassenbezeichnung zu ergänzen, um eine genaue Identifikation zwischen den verschiedenen Akteuren zu gewährleisten. Eine weitere Verarbeitung, seitens der Schule, erfolgt nicht, weshalb die Voraussetzung der DSGVO als erfüllt angesehen werden kann.

3. Datenminimierung

Mit dem vorherigen Punkt einhergehend wird auch die dritte Datenschutzregel erfüllt. Demnach müssen die personenbezogenen Daten „dem Zweck angemessen“ und „auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein“. Weitere, als die im Punkt (2) angegeben, persönlichen Daten sind nicht notwendig.

4. Richtigkeit und Korrektur

Die erforderlichen personenbezogenen Daten, zwecks Einrichtung des Office 365 Accounts, werden dem Anmeldebogen entnommen, welcher von jedem/jeder Schüler/in bei der Einschulung ausgefüllt werden muss. Es kann also davon ausgegangen werden, dass die Daten gemäß Art. 5 Abs. 1 lit. d DSGVO i. d. R.[8] sachlich richtig sind.
Sollten sich die personenbezogenen Daten zu einem späteren Zeitpunkt ändern, sich als unvollständig oder fehlerhaft darstellen, werden diese umgehend gelöscht oder berichtigt, wodurch neben dem Art. 5 Abs. 1 lit. d DSGVO auch dem Art. 16 DSGVO gerecht wird. Die Korrektur oder Löschung erfolgt durch die schulinterne Administration.

5. Speicherbegrenzung und Recht auf Vergessen

Die personenbezogenen Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es (...) erforderlich ist“. Dies bedingt auch das Recht auf Löschung bzw. Vergessenwerden.[11] Demnach müssen die personenbezogenen Daten unverzüglich gelöscht werden, sofern der Verarbeitungsweck, für die sie erhoben wurden, nicht mehr notwendig ist oder die betroffene Person ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO oder Art. 9 Abs. 2 DSGVO widerruft.
Dem Tatbestand wird gerecht, da mit dem IT-Dienstleister „Mr. Byte“ vertraglich vereinbart wurde, dass alle entsprechenden Daten nach Aufforderung gelöscht werden. Darüber hinaus werden auch die gespeicherten Daten bei der Microsoft Corporation gelöscht. In diesem Zusammenhang ist zwischen dem aktiven und dem passiven

[7] https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations?geo=UnitedStates#germany
[8] https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-iso-27001?view=o365-worldwide

Löschszenario zu unterschieden. Die passive Löschung tritt ein, sobald das Abonnement der Schule endet oder beendet wird. Dadurch werden alle in Office 365 gespeicherten Kundendaten, nach einem Aufbewahrungszeitrum von 180 Tagen, gelöscht. Die Löschung ist spätestens 90 Tagen danach vollständig abgeschlossen. Das aktiven Löschszenario wird durch die zuständigen Administratoren ausgelöst, immer wenn Nutzer/innen aus dem System ‚Schule' ausscheiden oder die Einwilligung widerrufen wird. Die persönlichen Daten und die Kundendaten respektive Kundeninhalte hinsichtlich Kennwörter, Zertifikate, Textdateien, Bilddateien etc., welche durch Dienste in Office 365 verwendet werden, sind nach Löschantrag durch den Administrator noch höchstens 30 Tage bei der Microsoft Corporation gespeichert. Die identifizierbaren Informationen, mit denen der Benutzer eines Microsoft-Diensts identifiziert oder verwendet werden kann, sind spätestens nach 180 Tagen vollständig gelöscht.[9]

6. Integrität und Vertraulichkeit

Es muss eine angemessene Sicherheit der relevanten Daten sichergestellt werden. Dies umfasst die Datensicherheit vor Verlust, Zerstörung oder Beschädigung sowie vor unbefugter bzw. unrechtmäßiger Verarbeitung.
Dies wird bspw. dadurch gewährleistet, dass der Zugang für Gäste zu dem schulinternen System unterbunden ist, wodurch keine außenstehenden Personen in das System nach Nutzer/innen suchen können. Alle Accounts sind durch individuelle Passwörter geschützt, die jede/r Nutzer/in selbst wählt. Diese Passwörter sind für die Administratoren der Schule sowie anderen Beteiligten unbekannt und können nicht eingesehen werden. Von der Nutzung von externen Apps, die nicht von der Schule vorgegeben werden, wird dringend abgeraten, da die Sicherheit und Vertraulichkeit der eigenen Daten nicht mehr gewährleistet werden kann.
Die Microsoft Corporation verspricht die personenbezogenen Daten der Nutzer/innen weder zu verkaufen noch zu verleihen. Auch die Verwendung für Werbezwecke oder ähnliche kommerzielle Zwecke wird ausgeschlossen.

Microsoft gibt an:
"*Für Microsoft-Produkte, die von Ihrer K-12 Schule* (Primär- und Sekundärbereich) *bereitgestellt werden, einschließlich Microsoft 365 Education, wird Microsoft:*

- *neben den für autorisierte Bildungs- oder Schulzwecke erforderlichen Daten keine personenbezogenen Daten von Schülern/Studenten erfassen oder verwenden,*
- *personenbezogene Daten von Schülern/Studenten weder verkaufen noch verleihen,*
- *personenbezogene Daten von Schülern/Studenten weder zu Werbezwecken noch zu ähnlichen kommerziellen Zwecken wie Behavioral Targeting von Werbung für Schüler/Studenten verwenden oder freigegeben,*
- *kein persönliches Profil eines Schülers/Studenten erstellen, es sei denn, dies dient der Unterstützung autorisierter Bildungs- oder Schulzwecke oder ist von den Eltern, Erziehungsberechtigten oder Schülern/Studenten im angemessenen Alter genehmigt, und*
- *seine Anbieter, an die personenbezogene Daten von Schülern/Studenten ggf. zur Erbringung der Bildungsdienstleistung weitergegeben werden, dazu verpflichten,*

[9] https://docs.microsoft.com/de-de/office365/enterprise/office-365-data-retention-deletion-and-destruction-overview

dieselben Verpflichtungen für personenbezogene Daten der Schüler/Studenten zu erfüllen."[10]

Verbleibendes Restrisiko:

Ein Restrisiko besteht bezüglich des als Cloud-Act bekannten Gesetzes aus den USA in Verbindung mit dem Privacy-Shield Abkommen zwischen den USA und der Europäischen Union, sowie dem sog. Schrems II-Urteil des EuGH aus dem Jahre 2020. Der „Cloud Act" regelt die Herausgabe von Daten an US-Behörden, auch wenn diese nicht in den USA, z. B. in Deutschland gespeichert sind.

Das Berufskolleg Kleve nimmt dieses latente Restrisiko ernst und sorgt dafür, dass auf Initiative des Berufskollegs keine Daten entstehen, die bei Herausgabe an US-Behörden, z. B. in Strafverfahren relevant sind. Auch Microsoft schützt die Kundendaten und geht gegen jede einzelne Anfrage gerichtlich vor.[11]

Ausführungen zusammengetragen von Thorben Broekmann, Fabian Dillhardt und Frank Janßen (Digitalisierungsbeauftragte bzw. Inhaber Stabsstelle Digitale Kommunikation, Information und Unterrichtsgestaltung)

[10] https://privacy.microsoft.com/de-de/privacystatement#mainnoticetoendusersmodule

[11] https://news.microsoft.com/de-de/im-daten-dschungel-wie-microsoft-mit-dem-cloud-act-umgeht/

11. Speicherorte für verschiedene Office 365 Dienste

Anmerkung: Die in den USA angesiedelten Microsoft Dienste Viva und Yammer sind Mitarbeitenden und Lernenden nicht zugänglich

Germany

▼ Click to expand

Service	Location
Exchange Online	Germany
OneDrive for Business	Germany
SharePoint Online	Germany
Microsoft Teams	Germany
Office Online & Mobile	Germany
EOP	Germany
Intune	European Union
Planner	European Union
Sway	United States
Yammer	European Union
OneNote Services	Germany
Stream	European Union
Whiteboard	European Union
Forms	European Union
Viva Connections	Germany
Viva Topics	Germany
Viva Learning	European Union
Viva Insights - Personal	Germany
Viva Insights - Manager/Leader AAD org data only	European Union
Viva Insights - Manager/Leader with 3rd party HR data only	United States
Viva Insights - Advanced	United States

Quelle:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?geo=UnitedStates%23germany&view=o365-worldwide#germany