dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Microsoft 365 im Bildungsbereich

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 44 360 99 99
datenschutz@dsb.zh.ch, datenschutz.ch

1 Einleitung

Dieser Leitfaden richtet sich an Schulen der obligatorischen und nachobligatorischen Schulstufen, der höheren Berufsbildung sowie an Hochschulen (nachfolgend Bildungsinstitutionen), die Microsoft 365 (nachfolgend M365) nutzen möchten. Er unterstützt die Projektleitung bei der datenschutzkonformen Einführung von M365.

Bei der Nutzung von M365 handelt es sich um eine Auslagerung (Bearbeiten im Auftrag im Sinne von § 6 Gesetz über die Information und den Datenschutz, IDG, LS 170.4). M365 enthält Applikationen, mit denen Informationen einer Bildungsinstitution nicht mehr auf den eigenen Servern oder den Servern eines Hosting-Anbieters, sondern in der Cloud von Microsoft bearbeitet und gespeichert werden (vgl. Auswahl von M365-Applikationen im Anhang).

2 Rechtliche Rahmenbedingungen

Die Auslagerung der Datenbearbeitung an Dritte ist möglich unter Beachtung der rechtlichen Rahmenbedingungen in § 6 IDG. So dürfen der Auslagerung keine rechtlichen Bestimmungen entgegenstehen und die Bildungsinstitution muss ihre Verantwortung für das Bearbeiten der Personendaten wahrnehmen können, auch wenn die Bearbeitung und Speicherung in einer Cloud erfolgt.

Siehe dazu Leitfaden Bearbeiten im Auftrag

2.1 Rechtsgrundlagenanalyse

Zu Beginn des Projekts ist eine Rechtsgrundlagenanalyse durchzuführen. In der Rechtsgrundlagenanalyse ist auch die Einhaltung von Geheimnispflichten (siehe Ziff. 2.3) und der Umgang mit dem CLOUD Act zu thematisieren (siehe Ziff. 2.4).

2.2 Klassifizierung der Daten

Eine Bildungsinstitution verfügt über die folgenden Arten von Daten, die von der Nutzung von M365 betroffen sein können und entsprechend zu klassifizieren sind.

Sachdaten	Informationen, die sich nicht auf bestimmte oder bestimmbare Personen beziehen Beispiele: Leere Arbeitsblätter, Saalpläne
Personendaten	Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen (§ 3 Abs. 3 IDG) Beispiele: Name, Vorname, Adresse, Zuteilung Schulklasse
Besondere Personendaten	Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht (§ 3 Abs. 4 IDG) Beispiele: Aufsätze mit Angaben zu Religion oder politischen Ansichten, Arztzeugnisse, Personaldossiers

2.3 Einhaltung von Geheimnispflichten

Die von den Bildungsinstitutionen bearbeiteten Personendaten können dem allgemeinen Amtsgeheimnis unterstehen (§ 8 Gemeindegesetz des Kantons Zürich, GG, LS 131.1 und Art. 320 Strafgesetzbuch, StGB, SR 311.0). Das allgemeine Amtsgeheimnis steht einer Auslagerung nicht entgegen. Voraussetzung für eine rechtskonforme Auslagerung der Bearbeitung von Daten unter dem Amtsgeheimnis ist die vertragliche Überbindung der Geheimnispflicht an den Auftragnehmer (siehe Ziff. 2.5).

Die von den Bildungsinstitutionen bearbeiteten Personendaten können auch dem Berufsgeheimnis (Art. 321 StGB) unterstehen. Dies ist beispielsweise bei schulärztlichen und schulpsychologischen Informationen der Fall. Berufsgeheimnisse stehen einer Auslagerung in die M365-Cloud entgegen, sofern die Auslagerung ein Offenbaren der Daten an Microsoft beinhaltet. Kann ein Auftragnehmer als Hilfsperson qualifiziert werden, liegt kein Offenbaren vor. Bei Unternehmen wie Microsoft beziehungsweise deren Mitarbeitenden liegt

keine Hilfspersoneneigenschaft vor. Die Nutzung von M365 kann jedoch durch technische oder organisatorische Massnahmen ermöglicht werden (siehe Ziff. 3).

2.4 Umgang mit dem CLOUD Act

Der CLOUD Act ist ein Gesetz der USA. Es ermöglicht bestimmten US-Behörden, amerikanische Unternehmen wie Microsoft zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, selbst wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Gelangt eine US-Behörde mit einer Anordnung zur Herausgabe von Personendaten an Microsoft, darf Microsoft unter Umständen die Bildungsinstitution nicht einmal über die entsprechende Anordnung informieren, und die Bildungsinstitution respektive die betroffenen Personen haben keine Verfahrensrechte.

Diese Zugriffsmöglichkeit ist aus datenschutzrechtlicher Sicht rechtswidrig. Deshalb dürfen Daten, die unter dem Berufsgeheimnis stehen, nur in der Cloud von Microsoft bearbeitet oder gespeichert werden, wenn technische Massnahmen eine einseitige Möglichkeit zur Kenntnisnahme durch Microsoft ausschliessen (siehe Ziff. 3.2). Alternativ können diese Daten bei der Nutzung von M365 im Rahmen einer hybriden Lösung ausserhalb der Microsoft-Cloud bearbeitet und gespeichert werden. Die Einhaltung der Trennung zwischen lokaler Bearbeitung und Cloud-Bearbeitung ist mit organisatorischen Massnahmen zu begleiten (siehe Ziff. 3.1).

Die Zugriffsmöglichkeit unter dem CLOUD Act führt bei der Risikoabwägung nach § 7 IDG dazu, dass Microsoft keinen Zugriff auf besondere Personendaten haben darf. Der Zugriff muss auch hier durch technische Massnahmen verhindert werden (siehe Ziff. 3.2). Alternativ können diese Daten im Rahmen einer hybriden Lösung ausserhalb der Microsoft-Cloud bearbeitet und gespeichert werden (siehe Ziff. 3.1).

2.5 Vertragsbeziehung mit Microsoft

Damit eine Auslagerung der Bearbeitung von Personendaten rechtmässig ist, muss ein datenschutzkonformer Vertrag mit dem Auftragnehmer abgeschlossen werden. Dieser Vertrag muss den Anforderungen von § 25 der Verordnung über die Information und den Datenschutz des Kantons Zürich (IDV, LS 170.41) genügen.

Educa hat mit Microsoft eine Rahmenvereinbarung für die Nutzung von M365 in Schulen der obligatorischen und nachobligatorischen Schulstufen sowie der höheren Berufsbildung abgeschlossen. Die Rahmenvereinbarung regelt wichtige datenschutzrechtliche Punkte. Weiter werden rechtliche Aspekte wie das anwendbare schweizerische Recht und der schweizerische Gerichtsstand geregelt.

Für Bildungsinstitutionen unter der Educa-Rahmenvereinbarung erfolgt die Beitrittserklärung, indem ein Microsoft-Volumenlizenzvertrag unterzeichnet wird, der beim für die Bildungsinstitution zuständigen Microsoft Lizenzpartner erhältlich ist. Die Bildungsinstitution muss explizit darauf hinweisen, dass eine Beitrittserklärung unter Inanspruchnahme der Educa-Rahmenvereinbarung gewünscht wird, sonst kommen die speziellen datenschutzrechtlichen Rahmenbedingungen nicht zum Tragen.

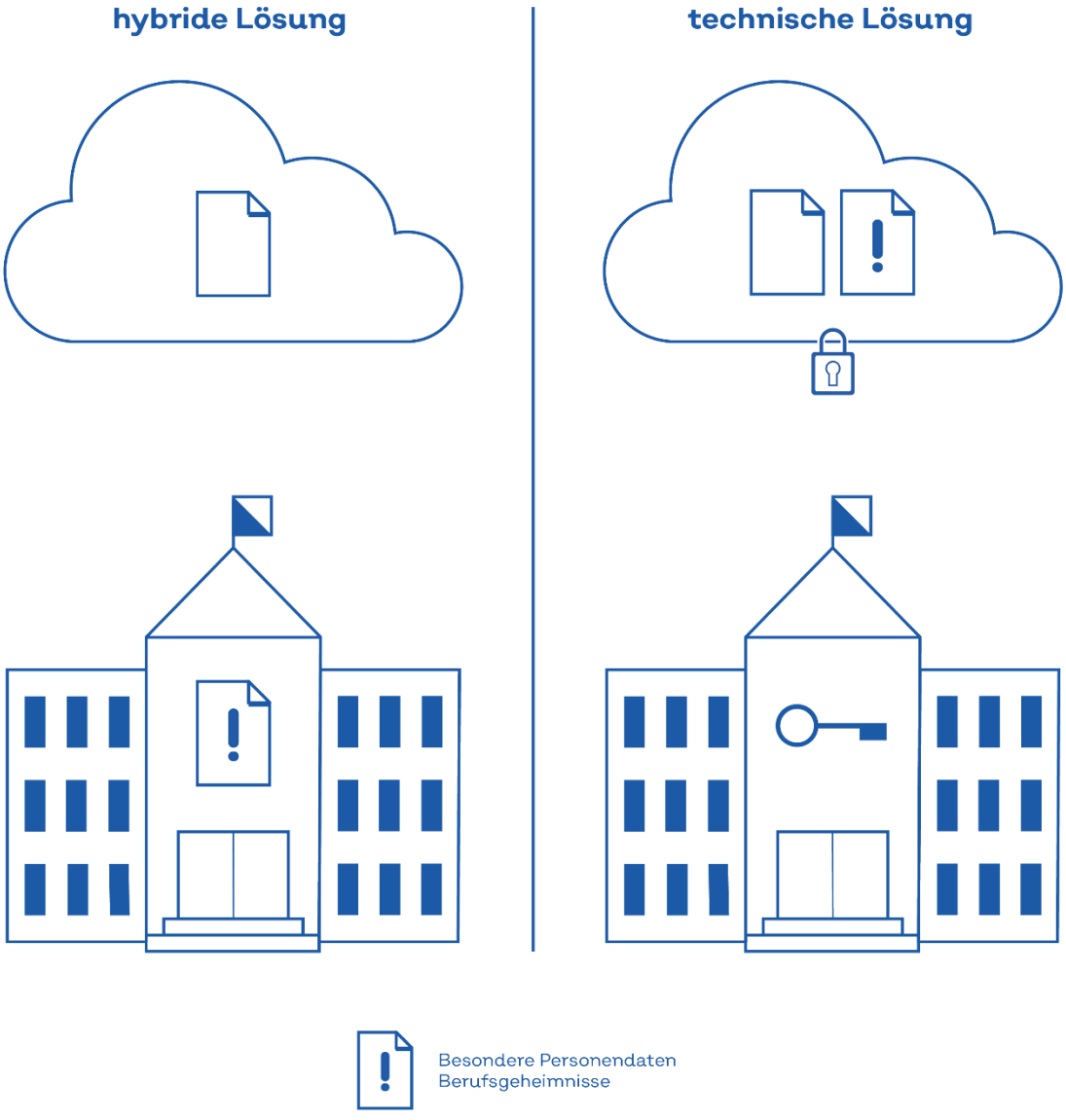
Für Institutionen der Tertiärstufe wie Universitäten, Pädagogische Hochschulen und Fachhochschulen besteht derzeit keine Rahmenvereinbarung. Für eine datenschutzkonforme Nutzung müssen sich Bildungsinstitution an Microsoft wenden und die gleichen datenschutzrechtlichen Punkte einfordern, inklusive Gerichtsstand Schweiz und anwendbarem schweizerischem Recht. Weitere Hinweise zur Vertragsgestaltung können dem Leitfaden Bearbeiten im Auftrag der Datenschutzbeauftragten entnommen werden.

Die direkte Anmeldung durch Schülerinnen und Schüler mit einer E-Mail-Adresse der Bildungsinstitution zur Nutzung von M365 ohne Unterzeichnung der entsprechenden Verträge ist nicht datenschutzkonform.

3 Varianten für die Nutzung von M365 für besondere Personendaten sowie für dem Berufsgeheimnis unterstehende Daten

Es gibt zwei Varianten, wie M365 genutzt werden kann, so dass Microsoft keinen Zugriff auf Berufsgeheimnisse und besondere Personendaten hat:

– Hybride Lösung, bei der die Daten unter dem Berufsgeheimnis und die besonderen Personendaten ausserhalb der Microsoft-Cloud bearbeitet und gespeichert werden
– Technische Lösung, die eine einseitige Kenntnisnahme dieser Daten durch Microsoft ausschliesst



3.1 Hybride Lösung

Werden bei der Nutzung von M365 keine technischen Massnahmen ergriffen, die die einseitige Kenntnisnahme durch Microsoft ausschliessen (siehe Ziff. 3.2), sind besondere Personendaten sowie Daten unter dem Berufsgeheimnis im Rahmen einer hybriden Lösung ausserhalb der Microsoft-Cloud zu bearbeiten und zu speichern. Sie können lokal bei der Bildungsinstitution oder bei einem Drittanbieter ohne US-Bezug bearbeitet und gespeichert werden.

Die Nutzung von M365 durch Mitarbeitende der Bildungsinstitution ist in einer Weisung oder Richtlinie zu regeln. Als Hilfestellung kann die Vorlage Weisung zur Informationssicherheit in Volksschulen genutzt werden. Zusätzlich ist in der Weisung festzuhalten, welche Arten von Daten mit welchen Microsoft-Applikationen bearbeitet werden dürfen (vgl. als Beispiel untenstehende Tabelle). Die Mitarbeitenden sind zur Weisung regelmässig zu schulen. Die Einhaltung der Weisung ist zu kontrollieren. Die Kontrollen sind zu dokumentieren.

Ein hybrider Betrieb ist mit den folgenden M365 Applikationen (Beispielauswahl) somit wie folgt möglich:

		Klassifizierung der Daten	Sachdaten	Personendaten	Besondere Personendaten	Besondere Amts-geheimnisse	Berufs-geheimnisse
Microsoft Applikationen	Office 365 Apps	Word / Excel / PowerPoint lokal	✔	✔	✔	✔	✔
	Office 365 Online	Word / Excel / PowerPoint in der Cloud	✔	✔	✖	✖	✖
	Exchange Mailserver	Lokal oder gehostet bei Dritten[1]	✔	✔	✔	✔	✔
		Online	✔	✔	✖	✖	✖
	Teams	Audio- oder Video-besprechungen ohne Aufzeichnung	✔	✔	✔	✔	✔
		Übrige Funktionen	✔	✔	✖	✖	✖
	Sharepoint		✔	✔	✖	✖	✖
	OneDrive		✔	✔	✖	✖	✖
	Copilot		✔	✔	✖	✖	✖

✔ Nutzung möglich ✖ keine Nutzung

Ausnahme: Werden Daten **einzelfallweise** mit DKE oder CASB gegenüber Microsoft verschlüsselt, können sie auch bei der hybriden Nutzung von M365 in der Microsoft Cloud bearbeitet und/oder gespeichert werden.

1 Unter Einhaltung der Anforderungen an die Auslagerung der Datenbearbeitung an Dritte.

Erläuterungen zur Tabelle:

– Gewisse M365-Applikationen werden ausschliesslich als Webversion angeboten und funktionieren nur online in der Microsoft Cloud. Darunter fallen namentlich Sharepoint, OneDrive, Copilot (vgl. Anhang, mit Stern markierte Applikationen). Aufgrund der Zugriffsmöglichkeit von US-Behörden gestützt auf den CLOUD Act können in diesen Applikationen deshalb keine besonderen Personendaten sowie dem Berufsgeheimnis unterstehende Daten bearbeitet werden (vgl. Ziff. 2.4).
– Die Applikation Exchange Online kann nur in der Microsoft-Cloud genutzt werden. Eine hybride Nutzung ist nicht möglich. Beim Erhalt von E-Mails kann nicht ausgeschlossen werden, dass besondere Personendaten sowie dem Berufsgeheimnis unterstehende Daten in der Microsoft-Cloud bearbeitet und gespeichert werden. Microsoft Exchange Online kann deshalb nicht datenschutzkonform genutzt werden ohne technische Massnahmen, die die einseitige Möglichkeit zur Kenntnisnahme durch Microsoft ausschliessen (siehe Ziff. 3.2).

3.2 Technische Lösung

3.2.1 Verschlüsselung

Es gibt zwei technische Massnahmen, die eine einseitige Kenntnisnahme der Daten durch Microsoft verhindern. Die umfassende Nutzung der Double Key Encryption (DKE) und die umfassende Nutzung eines Cloud Access Security Broker (CASB) mit Verschlüsselung gegenüber Microsoft.

- Bei der DKE von Microsoft werden Dokumente auf dem Gerät verschlüsselt, bevor sie in die Microsoft-Cloud geladen werden. Die Verschlüsselung erfolgt mit zwei Schlüsseln. Ein Schlüssel liegt bei Microsoft, der andere bei der Bildungsinstitution. Die Bildungsinstitution behält die vollständige Kontrolle über ihren Schlüssel (zum Schlüsselmanagement siehe Ziff. 3.2.2).
- CASB-Lösungen verschlüsseln den Datenfluss zwischen den Geräten der Bildungsinstitution und der Microsoft-Cloud. Die Daten werden verschlüsselt, bevor sie in der Microsoft-Cloud gespeichert werden. Microsoft hat damit keine Möglichkeit, einseitig auf Daten zuzugreifen (zusätzliche Massnahmen bei der Verwendung von CASB, siehe Ziff. 3.2.3).

Hinweise:

- Verschlüsselungslösungen wie Bring Your Own Key (BYOK) schliessen eine einseitige Kenntnisnahme durch Microsoft nicht aus. Bei BYOK wird der Schlüssel in der Microsoft-Cloud gespeichert. Microsoft kann sich also Zugriff auf den Schlüssel verschaffen und damit auf die verschlüsselten Daten.
- In der Applikation Teams kann eine Ende-zu-Ende-Verschlüsselung eingeschaltet werden. Audio- und Videodaten werden beim Sendenden verschlüsselt und beim Empfangenden entschlüsselt. Einige Funktionen wie das Aufzeichnen von Anrufen sind bei einer Ende-zu-Ende-Verschlüsselung nicht möglich.

3.2.2 Schlüsselmanagement

Es ist ein Kryptokonzept zu erstellen. Darin ist unter anderem festzuhalten:

- welche Verschlüsselungsverfahren warum verwendet werden
- wie die Schlüssel gesichert werden (Backup)
- wie Schlüssel erzeugt, gespeichert, ausgetauscht und wieder gelöscht werden
- wie die Integrität und Authentizität der Schlüssel sichergestellt werden
- wer Zugriff auf die Schlüssel hat. Dies kann auch im Rahmen des Rollen- und Berechtigungskonzepts abgehandelt werden (siehe Ziff. 4)

Weitere Informationen:

- BSI-Baustein CON.1 «Kryptokonzept»
- NIST-Guideline for Key-Management

3.2.3 Zusätzliche Massnahmen bei der Verwendung eines CASB

Eine CASB-Lösung kann lokal bei der Bildungsinstitution oder bei einem Dritten installiert werden. Ist die Lösung lokal installiert, hat nur die Bildungsinstitution Zugriff auf die Schlüssel und die Daten (siehe Ziff. 3.2.2). Ist die CASB-Lösung bei einem Dritten installiert, so kann er Zugriff auf die Schlüssel und damit auf die Daten haben. Entsprechend sind die Anforderungen an die Auslagerung der Datenbearbeitung an den Dritten zu beachten.

Weitere Informationen:

- Leitfaden Bearbeiten im Auftrag
- Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
- Leitfaden Auslagerung: CLOUD Act

4 Allgemeine Massnahmen bei der Nutzung von M365

Nach der Klärung der beschriebenen rechtlichen Rahmenbedingungen ist eine Risikoanalyse durchzuführen. Dazu dient ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept). Die Bildungsinstitution hat die spezifischen Risiken durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren (§ 7 IDG). Als Muster können die Vorlagen des Competence Center Projektmanagement des Kantons Zürich verwendet werden.

Das ISDS-Konzept muss unter anderem folgende Punkte umfassen:

- **Einstufung des Schutzobjekts:** Es ist eine Schutzbedarfsanalyse vorzunehmen (siehe Vorlagen).
- **Risikoanalyse und Schutzmassnahmen:** Darin sind die relevanten Risikofaktoren (Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit) aufzulisten, zu beschreiben, zu bewerten und mit entsprechenden Schutzmassnahmen zu minimieren (siehe Vorlagen).
- **Rollen- und Berechtigungskonzept:** Darin ist unter anderem festzulegen, welche Personengruppen auf welche Applikationen und welche Daten zugreifen dürfen (weitere Informationen: BSI-Baustein ORP 4 «Identitäts- und Berechtigungsmanagement» oder DSB-Vorlagen).
  - Beispielsweise bei Schulen: Lehrpersonen, Lernende, Fachpersonen, Schulpsychologinnen und Schulpsychologen, Schulpflege, Schulleitung, Schulsekretariat, Administratorin oder Administrator, Kursverwaltung usw.
  - Beispielsweise bei Hochschulen: Dozierende, Lehrpersonen, Studierende, Fachpersonen, Hochschulleitung, Hochschulrat, Administratorin oder Administrator usw.
- **Datensicherung und Notfallplanung:** Die Massnahmen zur Datensicherung und Notfallplanung sollten unter anderem einen zweiten, redundanten Internetanschluss, lokale Backups oder die Verwendung der Desktop-Version der Office-Programme beinhalten (siehe Vorlagen).

Die Nutzung von M365 setzt ein etabliertes und umfassendes Informationssicherheits- und Managementsystem (ISMS) der Bildungsinstitution voraus. Die Datenschutzbeauftragte stellt dafür Vorlagen zur Verfügung. Es sind insbesondere die Verantwortlichkeiten und die Schutzziele zu definieren sowie eine Risikoanalyse mit den entsprechenden Massnahmen durchzuführen. Das ISDS-Konzept für M365 ist in das übergeordnete ISMS zu integrieren und die Konformität zu den entsprechenden Vorgaben ist zu prüfen.

In diesem Leitfaden werden nur M365-spezifische Schutzmassnahmen erwähnt. Die sonstigen Schutzmassnahmen für IKT-Systeme sind zusätzlich umzusetzen. Dazu zählen die umfassende Nutzung eines Virenschutzes oder die regelmässige Schulung und Sensibilisierung der Mitarbeitenden.

4.1 Orientierung an internationalen Standards

Die Schutzmassnahmen für M365 orientieren sich an internationalen Standards. Dies sind beispielsweise:

- Bausteine OPS.2.2 Cloud-Nutzung und OPS.2.3 Nutzung von Outsourcing des Deutschen Bundesamtes für Informationssicherheit (BSI)
- Handbuch IT-Grundschutz Compliance für Office 365
- Sicherer Betrieb von M365 gemäss dem Center for Internet Security (CIS)

4.2 Konfigurationsmanagement

Die Konfiguration von M365 ist zu dokumentieren und regelmässig zu überprüfen. Microsoft führt laufend Updates durch, ändert Funktionen oder fügt neue hinzu. Diese Änderungen sind in der Microsoft-Roadmap ersichtlich. Hinweise auf mögliche Fehlkonfigurationen beziehungsweise Verbesserungen geben der sogenannte Secure Score von Microsoft, der CIS-Benchmark sowie interne und externe Audits. Zur korrekten Konfiguration von M365 gehört auch das Verwenden eines eigenen Domänennamens und eines etablierten Changemanagements.

Weitere Informationen:

- Microsoft 365 Change guide

4.3 Authentifizierung und Passwörter

Generell ist eine Multi-Faktor-Authentifizierung zu implementieren. Diese kann in M365 aktiviert werden – siehe Anleitung von Microsoft. Es können auch das TAN-Verfahren oder Einmalpasswörter eingesetzt werden. Müssen externe IT-Techniker regelmässig auf den Tenant der Bildungsinstitution zugreifen, ist der Einsatz des Privileged Identity Management zu prüfen.

Bei hohem Risiko ist die Aktivierung des bedingten Zugriffs mit Azure AD (Conditional Access) zu prüfen. Dabei können Zugriffe mit verschiedenen Parametern geregelt werden. So kann beispielsweise der Zugriff vor Ort in der Bildungsinstitution (z.B. im Klassenzimmer oder dem Vorlesungssaal) mit Nutzernamen, Kennwort und auf dem Computer gespeicherten Zertifikat erfolgen. Im Homeoffice wird zusätzlich ein dritter Faktor verlangt.

Weitere Informationen:
- Synchronisation von Identitäten und Authentifizierung bei M365
- Integration des lokalen Active Directory in Azure Active Directory
- Bedingter Zugriff mit Azure AD

4.4 Telemetriedaten

Die lokalen M365-Programme übermitteln Telemetriedaten an Microsoft. Diese Daten enthalten Personendaten in der Form von Informationen über die Mitarbeitenden und ihre Nutzung der M365-Applikationen. Es sind insbesondere folgende Vorkehrungen zu treffen:
- Bei den Diagnosedaten ist die Option «Weder noch» zu aktivieren.
- Die «optional verbundenen Erfahrungen» sind zu konfigurieren und zentral zu deaktivieren.
- Die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit ist zu deaktivieren (Microsoft Customer Experience Improvement Program, CEIP).

Weitere Informationen:
- Benchmark des Center for Internet Security (CIS) für Office-Programme

4.5 Länderauswahl

Bei der Nutzung von M365 sind die Länder zu bestimmen, in denen die bearbeiteten Daten gespeichert werden. Die Daten müssen in der Schweiz oder in der EU gespeichert werden (EU-Datengrenze für die Microsoft Cloud oder auch EU Data Boundary).

4.6 Deaktivierung von Microsoft Copilot

Microsoft Copilot ist in verschiedenen M365-Applikationen integriert. Der Dienst kann Inhalte erfassen, auswerten und zur KI-gestützten Erstellung von Texten oder Vorschlägen verwenden. Dadurch können besondere Personendaten und dem Berufsgeheimnis unterstehende Daten in Cloud-Diensten von Microsoft bearbeitet werden. Copilot ist deshalb in allen Anwendungen zu deaktivieren.

V 2.0 / Juli 2026

Anhang: Applikationen der M365 Produktpalette (Auswahl)

Die M365-Produktpalette wird regelmässig aktualisiert. Aktuell werden insbesondere folgende Applikationen angeboten:

- Advanced Threat Analytics
- Azure Active Directory*
- Azure Cloud Plattform*
- Bookings*
- Cloud App Security*
- Copilot*
- Delve*
- Dynamics 365
- Editor*
- Exchange Online*
- Forms*
- Groups*
- Intune*
- Lists*
- Loop*
- Microsoft 365 Apps for Enterprise
- Microsoft Defender (Portal*)
- Microsoft Secure Score*
- Microsoft Purview*
- Microsoft Mobile Apps
- Office 365 Plattform mit Office für das Web
- OneDrive for Business
- OneNote*
- Phone System
- Planner*
- PowerApps
- Power Automate
- PowerBI
- Project Online*
- SharePoint, SharePoint Online*
- Stream
- Sway*
- Syntex
- Teams
- To-Do
- Visio
- Viva Connections*
- Viva Insights*
- Viva Engage*
- Whiteboard; Whiteboard in Teams
- Windows 365 Cloud-PC *
- Weitere (…)

* Diese Applikationen sind ausschliesslich als Webapplikation verfügbar - ein lokaler Betrieb ist nicht möglich.