

Leitfaden

Office 365 im Bildungsbereich

Inhalt

1	Einleitung.....	2
2	Rahmenvertrag / Beitrittserklärung.....	2
2.1	Rahmenvertrag.....	2
2.2	Beitrittserklärung Volksschulen und Schulen der Sekundarstufe II	2
2.3	Beitrittserklärung Hochschulen.....	2
3	Konzept zur Nutzung von Office 365	3
3.1	Art der Nutzung	3
3.2	Auswahl der Dienste	3
3.3	Auswahl und Klassifizierung der Daten.....	3
3.4	Informationssicherheit	4
3.4.1	Verschlüsselung besonderer Personendaten	4
3.4.2	Protokollierung.....	5
3.4.3	Authentifizierung und Passwörter.....	5
3.4.4	Rollen- und Berechtigungskonzept	5
3.4.5	Löschen	6
3.4.6	Synchronisation von Daten mit Office 365	6
3.4.7	Datensicherung und Notfallplanung	6
4	Vom Berufsgeheimnis erfasste Daten.....	7
4.1	Datenzugriff mit Einwilligung	7
4.2	Verschlüsselung mit eigenem Schlüssel	7
5	E-Mail-Adressen	7
6	Länderauswahl	7
7	Schulung und Sensibilisierung	8
8	Information der Eltern	8
9	Anhang – Überblick Office 365-Dienste	9
9.1	Office 365-Dienste unter den Rahmenverträgen	9
9.2	Andere Dienste unter den Rahmenverträgen	10
9.3	Von den Rahmenverträgen nicht abgedeckte Dienste	11

1 Einleitung

Dieser Leitfaden richtet sich an Volksschulen, Schulen der Sekundarstufe II sowie an Hochschulen, die Office 365 nutzen wollen. Er gibt einen Überblick über die Vorgehensweise, Vorabklärungen und Massnahmen, die vor Inanspruchnahme und im Rahmen der Nutzung der Dienste umgesetzt werden müssen, um einen datenschutzkonformen Einsatz zu gewährleisten. Namentlich berücksichtigt wurden spezielle Risiken, die bei der Nutzung der Cloud für Datenbearbeitungen auftreten, sowie spezielle Massnahmen, die beim Bearbeiten von sensiblen, das heisst besonderen Personendaten umzusetzen sind.

2 Rahmenvertrag / Beitrittserklärung

2.1 Rahmenvertrag

Educa.ch hat mit Microsoft einen [Rahmenvertrag](#) für die Nutzung von Office 365 in den Primar- und Sekundarschulen sowie Schulen der Sekundarstufe II und Switch einen solchen für die Hochschulen unterzeichnet. Geregelt werden darin rechtliche Aspekte wie das anwendbare schweizerische Recht und der schweizerische Gerichtsstand. Microsoft verpflichtet sich, die Daten in europäischen Ländern zu speichern, namentlich in Irland und Holland.

Jede Schule, die diese Dienste nutzen will, muss zusätzlich eine Beitrittserklärung unterzeichnen. Die direkte Anmeldung durch Schülerinnen und Schüler mit einer E-Mail-Adresse der Schule zur Nutzung von Office 365 ohne Unterzeichnung der entsprechenden Verträge ist nicht datenschutzkonform.

2.2 Beitrittserklärung Volksschulen und Schulen der Sekundarstufe II

Für [Bildungseinrichtungen unter dem educa.ch-Rahmenvertrag](#) erfolgt die Beitrittserklärung, indem ein Microsoft-Volumenlizenzvertrag unterzeichnet wird, der beim für die Schule zuständigen Microsoft Authorized Education Partner erhältlich ist. Die Schule muss explizit darauf hinweisen, dass eine Beitrittserklärung unter Inanspruchnahme des [educa.ch-Rahmenvertrags](#) gewünscht wird, sonst kommen die speziellen datenschutzrechtlichen Rahmenbedingungen nicht zum Tragen.

2.3 Beitrittserklärung Hochschulen

Für Institutionen der Tertiärstufe wie Universitäten, Pädagogische Hochschulen und Fachhochschulen muss das Dokument «Beitritt für Bildungslösungen» von Microsoft unter Einbezug des Rahmenvertrags unterzeichnet werden. Dafür zuständig ist ein autorisierter Microsoft Licensing Solution Partner.

3 Konzept zur Nutzung von Office 365

Vor der Nutzung der Dienste ist ein Konzept zu erstellen, das alle wesentlichen Punkte betreffend die zukünftige Datenbearbeitung beinhaltet, insbesondere

- die Art der Nutzung
- das auf die Art der Nutzung abgestimmte Produkt
- die Art und der Umfang der zu bearbeitenden Daten
- die Verantwortlichkeiten
- die zum Schutz der Daten umzusetzenden Massnahmen wie Zugriffe, Verschlüsselung usw.

3.1 Art der Nutzung

Die Schule beziehungsweise die Schulleitung muss vor der Auswahl der Produkte entscheiden, zu welchen Zwecken sie die Dienste nutzen will respektive welche schulischen Aufgaben damit erledigt werden sollen. Sollen beispielsweise nur Arbeitsblätter gespeichert werden oder sollen die Schülerinnen und Schüler auch Hausaufgaben erledigen können? Es ist zu berücksichtigen, dass der Zweck die Auswahl bestimmt und nicht umgekehrt.

3.2 Auswahl der Dienste

Office 365 stellt eine Reihe von Diensten zur Verfügung (siehe Ziffer 9). Die Auswahl richtet sich nach den Bedürfnissen der Schule. Zu berücksichtigen ist, dass für das Bearbeiten von Personendaten nur diejenigen Dienste datenschutzkonform genutzt werden können, die vom Rahmenvertrag abgedeckt sind (siehe Ziffer 9.1 und 9.2).

3.3 Auswahl und Klassifizierung der Daten

Die Schule muss vorgängig für jeden gewählten Dienst festlegen, welche Daten bearbeitet werden sollen. Nicht alles, was möglich ist, ist erlaubt. Die Datenbearbeitung hat sich nach den schulischen Aufgaben und Zwecken zu richten. Es ist sicherzustellen, dass nur die Daten bearbeitet werden, die für die jeweilige Aufgabenerfüllung und den jeweiligen Zweck notwendig sind.

Das Lernverhalten darf grundsätzlich nicht überwacht und ausgewertet werden. Ausnahmen sind möglich, beispielsweise wenn das Produkt für eine Gruppenarbeit verwendet wird, die benotet wird.

Die Daten sind den folgenden Kategorien zuzuordnen, um nachfolgend die angemessenen Schutzmassnahmen bestimmen zu können:

Sachdaten	Informationen, die sich nicht auf Personen beziehen Beispiel: Arbeitsblätter
Personendaten	Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen Beispiel: Name, Vorname, Adresse
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 Beispiel: Resultat der schulärztlichen Untersuchung oder der schulpsychologischen Abklärung

3.4 Informationssicherheit

Die Schule muss technische und organisatorische Massnahmen umsetzen, um die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Daten zu gewährleisten. Je sensibler die Daten sind, umso umfassender sind die Informationssicherheitsmassnahmen. Dies gilt speziell für Daten, die dem Berufsgeheimnis unterliegen (siehe Ziffer 4). Insbesondere die folgenden Punkte sind zu berücksichtigen.

3.4.1 Verschlüsselung besonderer Personendaten

Sensitive, das heisst besondere Personendaten müssen [verschlüsselt](#) werden. Der Transport sowie die Speicherung der Daten sind bei Office 365 bereits verschlüsselt, wobei Microsoft über den Schlüssel verfügt.

Wenn Informationen den Bereich von Office 365 verlassen, beispielsweise beim Versand von E-Mails, stehen die folgenden Verschlüsselungsmechanismen zur Verfügung, wobei diese kostenpflichtig sein können. Die Verschlüsselung kann auf Stufe Dokument oder auf Stufe Office 365-Umgebung (Tenant) stattfinden:

- Dokument: Verschlüsselung der [Office-Datei](#) (Word, Excel, OneNote oder Powerpoint) selbst oder Verwendung eines [7-Zip-Archivs](#)
- Office 365-Umgebung: Verwendung eines eigenen Schlüssels ([Bring Your Own Key](#)) für die Verschlüsselung der Daten in Office 365. Dieser Schlüssel wird in einem Schlüsseltesor (Azure Key Vault) verwaltet und kann jederzeit von der Administratorin oder vom Administrator zurückgezogen werden (siehe auch Ziffer 4).

Die verwendeten Passphrasen und Schlüsselpaare sind sicher zu generieren und aufzubewahren, insbesondere bei der Verwendung eines eigenen Schlüssels.

3.4.2 Protokollierung

Bei der Nutzung der Dienste können Daten über die Nutzenden und deren Aktivitäten automatisch erfasst und gespeichert werden. Man spricht von Protokollieren respektive «Loggen». Diese Funktion muss jedoch von der Schule aktiviert werden.

Die Protokolldaten dürfen nur bearbeitet werden, wenn dies für das Funktionieren des Systems notwendig ist. Bei Verdacht auf Missbrauch der Dienste durch die Nutzenden können Protokolldaten stichprobenweise und nach vorgängiger Information der Betroffenen ausgewertet werden.

Weitere Informationen

- [Durchsuchen des Überwachungsprotokolls im Office 365 Security & Compliance Center](#)

3.4.3 Authentifizierung und Passwörter

Office 365 bietet grundsätzlich drei Arten der Authentifizierung:

- Verwendung der integrierten Office 365-Authentifizierung
- Synchronisation des Passworts aus dem internen Active Directory zu Office 365 (beziehungsweise Azure AD)
- Verwendung eines internen Active Directory Federation Service (ADFS)

Die Art der Authentifizierung ist im Rahmen einer Risikoanalyse zu bestimmen. Dabei sind der Zweck und der Umfang der Datenbearbeitung sowie die Art der bearbeiteten Daten zu berücksichtigen.

Für Administratorinnen und Administratoren oder wenn besondere Personendaten betroffen sind, ist eine Zwei-Faktor-Authentifizierung notwendig. Diese kann in Office 365 aktiviert werden und ist für Office 365-Produkte kostenlos. Die notwendigen Schritte werden [hier](#) erläutert. Es können aber auch das TAN-Verfahren oder Einmalpasswörter eingesetzt werden.

Passwörter dürfen nicht im Klartext sichtbar sein, müssen regelmässig geändert und verschlüsselt gespeichert werden.

Weitere Informationen

- [Synchronisation von Identitäten und Authentifizierung bei Office 365](#)
- [Integration des lokalen Active Directory in Azure Active Directory](#)

3.4.4 Rollen- und Berechtigungskonzept

Die Schule muss vor der Nutzung schriftlich in einem Rollen- und Berechtigungskonzept festlegen, welche Personengruppen (Lehrpersonen, Schülerinnen und Schüler, Fachpersonen, Schul-

psychologinnen und Schulpsychologen, Schulpflege, Schulleitung, Administratorin oder Administrator, Kursverwaltung usw.) auf welche Dienste und welche Daten zugreifen dürfen. Das Rollen- und Berechtigungskonzept ist regelmässig zu überprüfen.

Wird Customer Lockbox aktiviert, ist die verantwortliche Person im Berechtigungskonzept festzuhalten (siehe Ziffer 4).

3.4.5 Löschen

Das Löschen der Dokumente ist analog der Papierversion vorzunehmen. Lehrpersonen oder andere für die Löschung Verantwortliche können selbst löschen oder die Schülerinnen und Schüler beauftragen, entsprechende Verzeichnisse oder Dokumente nach den für die Schule geltenden Fristen zu löschen oder auf andere Speichermedien zu übertragen. Dieser Prozess lässt sich automatisieren. Die Automatisierung kann einfach gehalten oder sehr granular definiert werden. Die Administratorin oder der Administrator kann beispielsweise für die ganze Schule bestimmen, dass alle Dokumente nach einer bestimmten Frist gelöscht werden, falls sie nicht durch die Lehrpersonen bewusst verlängert wird.

Daten von Schülerinnen und Schülern oder Lehrpersonen, die ihr Konto nicht mehr nutzen, müssen durch die Schule gelöscht werden.

Die Löschung der Protokolldaten erfolgt automatisiert. Die Speicherfrist beträgt 90 Tage.

Weitere Informationen

- [Aufbewahren, Löschen und Zerstören von Daten in Office 365](#)

3.4.6 Synchronisation von Nutzerdaten mit Office 365

Für verschiedene Zwecke, beispielsweise für die Aktivierung der Office 365-Lizenz, müssen Daten mit Office 365 synchronisiert werden. Bei einer Synchronisation sind grundsätzlich nur diejenigen Nutzerdaten zu übermitteln, die für die Benutzung von Office 365 nötig sind. Es ist eine entsprechende Filterung im Synchronisationsdienst vorzunehmen.

Weitere Informationen

- [Azure AD Connect-Synchronisierung: Konfigurieren der Filterung](#)

3.4.7 Datensicherung und Notfallplanung

Die Anforderungen in Bezug auf die Verfügbarkeit von Office 365 sind zu definieren. Bei Bedarf sind entsprechende Massnahmen zur Datensicherung und Notfallplanung zu implementieren.

4 Vom Berufsgeheimnis erfasste Daten

Schulärztliche und schulpsychologische Informationen unterliegen dem Berufsgeheimnis. Solche Daten geniessen neben dem datenschutzrechtlichen auch strafrechtlichen Schutz. Dritte sollten keine oder nur unter besonderen Voraussetzungen Kenntnis dieser Daten erhalten, weshalb zusätzlich zu den in Ziffer 3 aufgeführten Massnahmen die folgenden Punkte zu berücksichtigen sind.

4.1 Datenzugriff mit Einwilligung

Bei der Nutzung von Office 365-Diensten ist eine Grundverschlüsselung für den Transport und die Speicherung implementiert. Microsoft verfügt jedoch über den Schlüssel. Deshalb muss der [Customer-Lockbox-Prozess](#) aktiviert werden. Dadurch wird sichergestellt, dass Microsoft in Supportfällen nur auf explizite Anfrage und nach expliziter Einwilligung der Administratorin respektive des Administrators auf die Daten zugreifen kann.

Customer Lockbox ist kostenpflichtig. Die für diesen Prozess verantwortliche Person ist im Rollen- und Berechtigungskonzept festzuhalten.

4.2 Verschlüsselung mit eigenem Schlüssel

Schulen, die über eine gewisse Grösse, eine geeignete IT-Infrastruktur respektive technisches Know-how verfügen, können für die Daten in Office 365 einen [eigenen Schlüssel](#) (Bring Your Own Key) implementieren. Der Schlüssel kann jederzeit von der Administratorin respektive vom Administrator zurückgezogen werden.

Dieser Schlüssel wird in einem Schlüsseltresor (Azure Key Vault) durch Microsoft verwaltet. Aus diesem Grund muss zusätzlich der [Customer-Lockbox-Prozess](#) aktiviert werden (siehe Ziffer 4.1).

5 E-Mail-Adressen

Müssen E-Mail-Adressen vergeben werden, sollten abgekürzte Namen oder Pseudonyme verwendet werden. Pseudonyme erschweren den Missbrauch der Konten durch Dritte.

Kann die Pseudonymisierung nicht selbst durchgeführt werden, bieten externe Dritte Lösungen für die Verwendung von Office 365 mit einem Pseudonym an. Bei Verwendung eines solchen Dienstes sind die Aspekte einer Auslagerung ebenfalls zu beachten.

6 Länderauswahl

Bei der Inanspruchnahme einzelner Dienste ist eine Länderauswahl zu treffen. Die Speicherorte müssen so gewählt werden, dass die Daten nur in Ländern mit angemessenem Datenschutzniveau, also vorzugsweise in der Schweiz (geplant ab 2019) oder in Europa gespeichert werden.

Eine Übersicht über die Speicherorte finden Sie [hier](#).

7 Schulung und Sensibilisierung

Alle Personen, die mit diesen Diensten Daten bearbeiten, müssen instruiert werden, wie jeder Dienst genutzt werden kann und soll. Schülerinnen und Schüler sind umfassend über die Art des Bearbeitens durch die Schule und darüber, wie sie Office 365 rechtmässig nutzen können, zu informieren.

8 Information der Eltern

Im Sinne der Transparenz sind die Eltern über diese neue Art der Datenbearbeitung im Rahmen der Volksschule zu informieren. Einerseits sind im Netz Rückschlüsse auf die Schülerinnen und Schüler möglich, beispielsweise durch E-Mail-Adressen, welche den Namen mit der Schule verbinden, andererseits nutzen die Schülerinnen und Schüler das Internet für die Schule auch zu Hause.

9 Anhang – Überblick Office 365-Dienste

9.1 Office 365-Dienste unter den Rahmenverträgen

Dienst	Beschreibung	Online	On premise
OneNote	Notizprogramm für Lehrpersonen Beispiel: elektronisches Verteilen von Arbeitsblättern	x	x
OneNote Class Note- book	Das OneNote-Kursnotizbuch bietet Zusatzfunktionen zu OneNote. Beispiele: Verteilen von Arbeitsblättern an Lernende, vereinfachtes Korrigieren von Hausaufgaben	x	
Exchange	Mail, Kalender, Aufgaben	x	x
SharePoint SharePoint Online	Speicherort für Dokumente für Teamdokumente	x	x
OneDrive for Business	Dokumentenspeicher für eigene Dokumente	x	x
Skype for Business	Telefonie, Chatten, Videokonferenzen, Screen und Application Sharing usw. Telefongespräch wird nicht gespeichert, nur Chat (auf dem Exchange Server). Videogespräche können aufgenommen und auf SharePoint gespeichert werden.	x	x
Teams	Chat-basierte Arbeitsumgebung in Office 365 Zusammenzug von Office 365-Diensten, mit starkem Fokus auf Teaminteraktion Beispiel: Kombination von Skype, SharePoint und OneNote	x	
Forms	Formular-Tool Beispiel: Lernkontrolle; zeigt an, was falsch ist.	x	
Delve	Analysiert und visualisiert die eigene Nutzung und bringt innerhalb von Office 365 für die Nutzenden interessante Dokumente und Informationen an die Oberfläche.	x	
Groups	Erlaubt unter anderem, in Outlook Gruppen von Personen zu bilden, mit denen E-Mails, Kalender, Dokumente usw. geteilt werden können.	x	
Project	Umfangreiches Projektmanagement-Tool	x	x

Planner	Teamarbeitstool für Tätigkeiten wie Pläne erstellen, Aufgaben organisieren und zuweisen, Dateien freigeben, Aufgaben im Chat besprechen und sich austauschen	x	
Stream	Video speichern, durchsuchen, teilen	x	
Flow	Geschäftsprozessautomatisierungstool zum Erstellen von automatisierten Workflows zwischen Apps und Diensten, um Benachrichtigungen zu erhalten, Dateien zu synchronisieren, Daten zu erfassen usw.	x	
PowerApps	Ermöglicht das Erstellen von benutzerdefinierten Business-Apps.	x	
PowerBI	Business Intelligence Zusammenzug von Tools zur Analyse und Visualisierung von Daten, die auf SharePoint gespeichert sind, und zum Teilen der Resultate	x	

9.2 Andere Dienste unter den Rahmenverträgen

Dienst	Beschreibung	Online	On premise
Azure Cloud Platform	Infrastructure as a Service (IaaS): Virtuelle Maschinen, Netzwerk, Storage Platform as a Service (PaaS): Datenbanken, Intelligence and Analytics Software as a Service (SaaS): Business Apps	x	
EMS E3 für Intune	Komponente zur Steuerung von Identitäten und Zugriffen in der Cloud, Verwaltung von mobilen Geräten und Apps Beispiel: Sicherstellen, dass alle Notebooks der Schule auf dem neusten Stand und vor unberechtigtem Zugriff geschützt sind.	x	
Microsoft Intune	Verwaltung von Apps und Geräten Teil der Enterprise Mobility Suite (EMS)	x	
Dynamics 365	Customer Relationship Management (CRM) und Enterprise Resource Planning (ERP) Dienst zum Verwalten von Ressourcen wie Buchhaltung, Lagerbewirtschaftung, Mitarbeitende, Lernende, Verträge etc. Beispiel: Übersicht, wann Kunden angerufen haben.	x	

9.3 Von den Rahmenverträgen nicht abgedeckte Dienste

Dienst	Beschreibung	Online	On premise
Sway	Online-Präsentationserstellungstool, das wie eine Website funktioniert. Daten werden ausserhalb der EU gespeichert. Kann nicht datenschutzkonform genutzt werden.	x	
Yammer	Social Media für Unternehmen Daten werden ausserhalb der EU gespeichert. Kann nicht datenschutzkonform genutzt werden.	x	
OneDrive (Consumer)	OneDrive kann im Gegensatz zu OneDrive for Business von Schulen nicht datenschutzkonform genutzt werden.	x	
Skype (Consumer)	Skype kann im Gegensatz zu Skype for Business von Schulen nicht datenschutzkonform genutzt werden.	x	

dsb



datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh