

Glarus, 13. Mai 2019

Merkblatt zu Office 365 für Schulen

Dieses Merkblatt richtet sich an die Schulleitungen, Lehrpersonen, Schuldienste und Schulbehörden die Office 365 nutzen. Es verweist auf den Rahmenvertrag zwischen educa.ch und Microsoft sowie das Dokument Amtsgeheimnis und Datenschutz, Aufbewahren von Daten des Departements Bildung und Kultur Kanton Glarus. Es leitet sich inhaltlich aus den Merkblättern des Datenschutzbeauftragten des Kantons Zürich ab, wurde jedoch an den Kanton Glarus angepasst.

Inhaltsverzeichnis:

1.	Rahmenvertrag educa.ch /Microsoft	2
2.	Nutzung von Office 365.....	2
2.1.	Art der Nutzung	2
2.2.	Art und Umfang der zu bearbeitenden Daten.....	2
2.3.	Datensicherheit	3
2.3.1.	Verschlüsselung besonders schützenswerter Personendaten	3
2.3.2.	Protokollierung	3
2.3.3.	Authentifizierung und Passwörter	3
2.3.4.	Rollen- und Berechtigungskonzept	4
2.3.5.	Löschen.....	4
2.3.6.	Synchronisation von Nutzerdaten mit Office 365	4
2.3.7.	Datensicherung und Notfallplanung.....	4
2.3.8.	Weitere Merkmale	4
3.	Schulung und Sensibilisierung	5
4.	Information der Eltern	5
5.	Anhang – Überblick Office 365-Dienste	5
5.1.	Office 365 Dienste unter den Rahmenverträgen.....	5
5.2.	Andere Dienste unter den Rahmenverträgen	7
5.3.	Von den Rahmenverträgen nicht abgedeckte Dienste.....	7

1. Rahmenvertrag educa.ch / Microsoft

Der Kanton Glarus sowie die drei Gemeinden Glarus, Glarus Nord und Glarus Süd verweisen auf den Rahmenvertrag für die Nutzung von Office 365 in den Primar- und Sekundarschulen I sowie an Schulen der Sekundarstufe II. 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. Die Gemeinden und der Kanton haben mit Softwareone (Microsoft Authorized Education Partner Microsoft) Microsoft-Volumenlizenzverträge unterzeichnet.

Weitere Informationen:

- <https://www.educa.ch/de/rahmenvertraege/teilnahmeberechtigung>
- <https://www.educa.ch/de/rahmenvertraege/microsoft>

2. Nutzung von Office 365

2.1. Art der Nutzung

Die Schule muss 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. Demzufolge sollten zur Nutzung der Dienste die Schulen die wesentlichen Fragen betreffend die zukünftige Datenbearbeitung beantworten können:

- Welche Dienste von Office 365 werden für organisatorische Zwecke genutzt?
- Welche Aufgaben werden mit diesen Diensten erledigt?
- Welche Dienste von Office 365 werden für unterrichtsrelevante Zwecke genutzt?
- Welche Aufgaben werden mit diesen Diensten erledigt?

Hinweise dazu:

- Es ist zu berücksichtigen, dass der Zweck die Auswahl bestimmt und nicht umgekehrt.
- Office 365 stellt eine Reihe von Diensten zur Verfügung (siehe Kapitel 5). 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 Kapitel 5).
- Das Lernverhalten darf grundsätzlich nicht überwacht und ausgewertet werden. Ausnahmen sind möglich, beispielsweise wenn das Produkt für eine Gruppenarbeit verwendet wird, die benotet wird.

2.2. Art und Umfang der zu bearbeitenden Daten

Um angemessene Schutzmassnahmen von Daten bestimmen zu können, muss die Schule diese nach folgenden Kategorien zuordnen (siehe auch Dokument Amtsgeheimnis und Datenschutz, Aufbewahren von Daten):

Sachdaten	Informationen, die sich nicht auf Personen beziehen. Beispiel: Arbeitsblätter
Personendaten	Informationen, die sich auf bestimmte oder bestimmbar Personen beziehen. Beispiel: Name, Vorname, Adresse

Besonders schützenswerte 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.
--	---

2.3. Datensicherheit

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 Datensicherheitsmassnahmen. Dies gilt speziell für Daten, die dem Amtsgeheimnis unterliegen (siehe Dokument Amtsgeheimnis und Datenschutz, Aufbewahren von Daten (DBK)). Insbesondere die folgenden Punkte sind zu berücksichtigen.

2.3.1. Verschlüsselung besonders schützenswerter Personendaten

Sensitive, das heisst besonders schützenswerte 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, oder zusätzlicher Schutzbedarf besteht, können Verschlüsselungsmöglichkeiten anderer, teils kostenpflichtiger Anbieter gewählt werden.

2.3.2. 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](#)

2.3.3. 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 besonders schützenswerte 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](#)

2.3.4. Rollen- und Berechtigungskonzept

Die Schule muss schriftlich in einem Rollen- und Berechtigungskonzept festlegen, welche Personengruppen (Lehrpersonen, Schülerinnen und Schüler, Fachpersonen, Schulleitung, Administratorin oder Administrator, Kursverwaltung usw.) auf welche Dienste und welche Daten zugreifen dürfen. Das Rollen- und Berechtigungskonzept ist regelmässig zu überprüfen.

2.3.5. 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](#)

2.3.6. 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](#)

2.3.7. 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.

2.3.8. Weitere Merkmale

Dieses Merkblatt verweist auf weitere Positionen, welche im Dokument Amtsgeheimnis und Datenschutz, Aufbewahren von Daten - Merkblatt für Schulleitungen, Lehrpersonen, Schulleitungen und Schulbehörden des Departements Bildung und Kultur Kanton Glarus aufgeführt sind.

3. 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.

4. 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.

5. Anhang – Überblick Office 365-Dienste

5.1. Office 365 Dienste unter den Rahmenverträgen

Die Tabelle ist in regelmässigem Abstand auf Aktualität zu überprüfen.

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	

5.2. 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	

5.3. 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	