Kanton Bern
Canton de Berne

Bildungs- und Kulturdirektion
Amt für Kindergarten, Volksschule und Beratung
Regelschulen Deutsch

MERKBLATT MICROSOFT 365

Inhaltsverzeichnis

1 Einleitung

Dieses Merkblatt richtet sich an die verantwortlichen Stellen von Volksschulen, die das Produkt «Microsoft 365» als Dienstleistung nutzen wollen (Software as a Service). Es vermittelt ihnen einen groben Überblick über die Vorgehensweise, über nötige Vorabklärungen und über Massnahmen, die zu ergreifen sind, um «Microsoft 365» möglichst datenschutzkonform zu nutzen. Namentlich berücksichtigt werden Risiken, die bei der Nutzung der Cloud für Datenbearbeitungen auftreten, sowie Massnahmen, die zu treffen sind, wenn besonders schützenswerte Personendaten bearbeitet werden.

Das Merkblatt ist eine Ergänzung zum Datenschutzlexikon des Kantons Bern.

2 Verantwortlichkeiten

Die Gemeinde trägt die alleinige Verantwortung für den Einsatz der angestrebten Infrastruktur mit Microsoft 365 in ihrer Schule. Die kommunale Datenschutzaufsichtsstelle der Gemeinde prüft das Konzept und veranlasst unter Umständen Verbesserungen.
Die kommunale Datenschutzaufsichtsstelle kann sich mit datenschutzrechtlichen Fragen an die kantonale Datenschutzaufsichtsstelle wenden.

3 Vertragliche Ebene

Durch die Nutzung von Microsoft 365 in der Volksschule entstehen für die verantwortlichen Behörden erhöhte Risiken im Bereich des Datenschutzes[1].

Ein wichtiges Instrument, um diese Risiken zu minimieren, ist der Educa-Rahmenvertrag, der Schweizer Recht mit Schweizer Gerichtsstand und die Wahl der Serverstandorte in der Europäischen Union oder in der Schweiz regelt.

Trotz des Rahmenvertrags verbleiben im Zusammenhang mit der Bearbeitung von besonders schützenswerten Daten und der von Microsoft erhobenen Randdaten bestimmte Risiken. Diese können unter Umständen durch aufwendige technische Massnahmen beseitigt werden. Andere Risiken hingegen lassen sich nicht beseitigen oder allenfalls nur minimieren. Diese bleiben als sogenannte Restrisiken bestehen. Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

Es gilt zu beachten, dass die vertraglichen Regelungen, insbesondere die Vertragsdauer, periodisch geprüft und allfällige Erneuerungen entsprechend geplant werden. Dies gilt auch für die von educa ausgehandelten Rahmenverträge.

4 Konzept

Bevor Microsoft 365 implementiert und genutzt wird, ist ein Konzept zu erstellen, das die Inhalte der Kapitel 4.1 bis 6 regelt – insbesondere die beabsichtigte Bearbeitung von Daten und die vorgesehenen Schutzmassnahmen [2].

[1] vgl. das überarbeitete privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen»: Überarbeitetes privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» – privatim
[2] Die Schulinformatik der PHBern unterstützt die Schulen in der Erarbeitung eines Cloudkonzepts.

Folgende Punkte sind dabei zentral:

- Nutzungsszenarien

  Welche Daten sollen für welchen Zweck auf welche Art und Weise bearbeitet werden?
- Klassifizierung der Daten

  Bestimmung des Schutzbedarfs der eruierten Daten
- Auswahl der geeigneten Dienste

  Mit welchen Microsoft-Diensten will die Schule welche Nutzungsszenarien umsetzen?
- Risiken erkennen und Schutzmassnahmen treffen

  Welchen Risiken ist die Personendatenbearbeitung ausgesetzt?
  Mit welchen angemessenen Massnahmen können diese Risiken beseitigt oder zumindest minimiert werden
- Restrisiken ausweisen

Bestimmte Risiken verbleiben bzw. können trotz Massnahmen nicht beseitigt werden. Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

4.1 Nutzungsszenarien

Die Nutzungsszenarien für Microsoft 365 stellen den Kern des Konzepts dar. Sie beschreiben die Bedürfnisse der Schule in Bezug auf die Digitalisierung. Sollten sich nach der Implementierung von Microsoft 365 weitere Bedürfnisse zeigen, muss das Konzept überarbeitet werden.

Die Nutzungsszenarien sollen mit allen beteiligten Personengruppen der Schule erarbeitet werden.

Folgende Punkte sollen in der Erarbeitung berücksichtigt werden:

- Nutzungsszenario im Rahmen der gesetzlichen Aufgabenerfüllung der Schule
  - Vorgängig muss die Zweckbindung geklärt werden
    - Beispiel für eine **legitime** Zweckbindung: *«Die Lehrperson hält fest, was sie bei einer Schülerin oder einem Schüler beobachtet.»*
    - Beispiel für eine **nicht** legitime Zweckbindung:
      «Alle Lehrpersonen einer Klasse wollen über die Lernstände der Schülerinnen und Schüler in sämtlichen Fachbereichen informiert sein.»
- Involvierte Personengruppen / Betroffene festhalten
- Die daraus resultierenden Produkte/Daten

Beispiel einer Zusammenstellung von Nutzungsszenarien mit Zweckbindung (nicht abschliessend):

	Szenario	**Betroffene**	**Produkte/Daten**
1	Ergebnisse von Einzel- oder Gruppenarbeiten (kooperative Arbeitsformen) OHNE Personenbezug	Schülerinnen und Schüler, Lehrpersonen	Website, Dokument, Ton- und Videoaufnahmen
2	Durchführung von Lernkontrollen	Schülerinnen und Schüler, Lehrpersonen	Dokumente, Tabellen (Auswertung)

3	Informationen an Eltern der Klasse (Klassenlager, Schulanlässe usw. …)	Schulleitung, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail
4	Kontaktdaten der Eltern erfassen (Telefon, Mail) und der Klasse, den Lehrpersonen wie auch den Erziehungsberechtigten zugänglich machen.	Schülerinnen und Schüler, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail
5	Dokumentieren des Mitarbeitergesprächs	Schulleitung, Lehrpersonen	Dokument
6	Erstellen von Förderplänen im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen im Regelschulangebot (MR, ehemals IBEM).[3]	Lehrpersonen, Klassenlehrperson, Erziehungsberatung, Erziehungsberechtigte	Dokumente, Mail

4.2 Klassifizierung der Daten - Bestimmung des Schutzbedarfs

Mithilfe eines Klassifizierungsprozesses ermitteln die Schulen, wie hoch der Schutzbedarf der Daten ist. Dabei werden folgende Ziele verfolgt:

- Grundlage für die Sensibilisierung bei den Nutzenden (Schulungen)
- Eruierung der zu untersuchenden Szenarien mittels einer Risikomatrix
- Eruierung des Schutzbedarfs von Daten ohne Personenbezug

Das Ampelsystem der PHBern[4] kann für die Kategorisierung von Daten eine Hilfestellung sein.

Die Produkte/Daten der einzelnen Szenarien werden analog der KRGV[5] wie folgt klassifiziert:

Schutzbedarf	Klassifizierung	Beschreibung
kein Schutzbedarf	Öffentlich	Diese Kategorie beschreibt Sachdaten wie zum Beispiel Unterrichtsmaterialien ohne Personenbezug, anonymisierte Personendaten.
normaler Schutzbedarf	Intern	In dieser Kategorie werden normale Personendaten erfasst. Beispiele: Vorname, Name, Mailadresse etc.
hoher Schutzbedarf	Vertraulich	Ein hoher Schutzbedarf besteht bei besonders schützenswerten Personendaten oder auch bei umfangreichen Sammlungen von normalen Personendaten und Persönlichkeitsprofilen. Beispiele: Krankheiten, Straftaten, Notfall-Klassenliste mit weiteren Telefonnummern und evtl. mit Informationen zu Krankheiten, Klassenübersicht mit beurteilungsrelevanten Daten. Ebenfalls können auch Sachdaten betroffen sein, die unter Berufs- oder Amtsgeheimnis stehen.

Beispiel einer Klassifizierung im Konzept:

	Szenario	Betroffene	Produkte/Daten	Klassifizierung
1	Ergebnisse von Einzel- oder Gruppenarbeiten (kooperative Arbeitsformen) OHNE Personenbezug	Schülerinnen und Schüler, Lehrpersonen	Website, Dokument, Ton- und Videoaufnahmen	Öffentlich
2	Durchführung von Prüfungen/Tests inklusive Beurteilung	Schülerinnen und Schüler, Lehrpersonen	Dokumente, Tabellen (Auswertung)	Vertraulich

[3] vgl. die VMR, https://www.belex.sites.be.ch/data/432.271.1/de/
[4] https://kibs.ch/datenschutz/ampelsystem
[5] Verordnung vom 13. März 2013 über die Klassifizierung, die Veröffentlichung und die Archivierung von Dokumenten zu Regierungsratsgeschäften (Klassifizierungsverordnung, KRGV; BSG 152.17).

3	Informationen an Erziehungsberechtigte der Klasse (Klassenlager, spezielle Anlässe…)	Schulleitung, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail	Intern
4	Kontaktdaten der Erziehungsberechtigten erfassen (Telefon, Mail) und der Klasse, den Lehrpersonen wie auch den Erziehungsberechtigten zugänglich machen. Nicht im Sinne einer Liste von Krankheiten oder Allergien.	Schülerinnen und Schüler, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail	Intern
5	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse	Schülerinnen und Schüler, Lehrpersonen	Dokument	Intern
6	Dokumentieren des Mitarbeitergesprächs	Schulleitung, Lehrpersonen	Dokument	Vertraulich
7	Erstellen von Förderplänen im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen im Regelschulangebot (MR, ehemals IBEM).[6]	Lehrpersonen, Klassenlehrperson, Erziehungsberatung, Erziehungsberechtigte	Dokumente, Mail	Vertraulich
8	Die Nutzenden vergessen ihr Passwort	Alle Nutzerinnen und Nutzer	Daten	Intern

Einzelne Produkte in Zusammenspiel mit den Szenarien der Betroffenen können unterschiedlich klassifiziert werden.

Beispiel:

	Szenario	Betroffene	Produkte	Klassifizierung
5.a	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse	Schülerinnen und Schüler, Lehrpersonen	Dokument	intern
5.b	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse (Integration einer Schülerin / eines Schülers mit visuell erkennbaren Beeinträchtigungen)	Schülerinnen und Schüler, Lehrpersonen	Dokument	vertraulich

4.3 Auswahl der geeigneten Dienste

Microsoft 365 bietet eine breite Palette von Diensten. Die Auswahl der Dienste richtet sich nach den Bedürfnissen der Schule (Kapitel 4.1). Es sollen nur Dienste genutzt werden, die vom Educa-Rahmenvertrag abgedeckt werden.

[6] vgl. die VMR, https://www.belex.sites.be.ch/data/432.271.1/de/

Weiter gilt zu beachten, dass Personendaten der Kategorie «*Vertraulich*» aufgrund der bestehenden Risiken in der Regel nicht mit Diensten von Microsoft 365 bearbeitet werden sollen. Hierfür sind im Konzept andere Fachapplikationen zu berücksichtigen, die für die Bearbeitung vertraulicher Daten geeignet sind.

Die im Kapitel 4.6 beschriebenen Möglichkeiten zur Verschlüsselung können eine Bearbeitung von Personendaten der Kategorie «*Vertraulich*» in Microsoft 365 ermöglichen.

Beispiel einer Dienstauswahl im Konzept:

Datenklassifizierung	gewählte Dienst
öffentlich & intern	Microsoft 365 Word, PowerPoint, Excel, OneDrive, Teams, Outlook
vertraulich	Beurteilung Kanton Bern[7] (keine Vorabkontrolle durch Gemeinde nötig) Lehreroffice, Tresorit, Protonmail, Klapp, Threema, Scolaris und andere (Vorabkontrolle durch Gemeinde nötig)

4.4 Risiken erkennen und Schutzmassnahmen treffen

Die Nutzungsszenarien und die daraus resultierenden Produkte/Daten werden unter Berücksichtigung der Klassifizierung auf realistische Risiken hin untersucht. Szenarien mit Produkten/Daten der Kategorie «*Öffentlich*» müssen nicht überprüft werden.
Bei der Kategorie «*Vertraulich*» sind erhöhte Anforderungen an den Schutz der Vertraulichkeit der Daten zu stellen und in der Risikoabwägung zu berücksichtigen. Die verantwortliche Behörde kann beispielsweise aufwendige technische Massnahmen miteinbeziehen (behördenseitige Verschlüsselung) und so eine Bearbeitung dieser Kategorie ermöglichen.

Die folgende Risikomatrix verdeutlicht, welche Risiken durch zusätzliche Schutzmassnahmen minimiert werden müssen.
Die Ziffern der Achse «Eintrittswahrscheinlichkeit» werden mit den Ziffern «Auswirkung / Schadensausmass» multipliziert. Die Ergebnisse können in der Regel wie folgt gelesen werden:

- 1 und 2: Keine Massnahmen
- 3 – 6: Technische und organisatorische Massnahmen.
- 8 – 16: Wahl einer spezifischen Fachapplikation oder weitergehende technische und schulorganisatorische Massnahmen.

Eintrittswahrscheinlichkeit					
	4 sicher	4	8	12	16
	3 sehr wahrscheinlich	3	6	9	12
	2 wahrscheinlich	2	4	6	8
	1 unwahrschienlich	1	2	3	4
		1 unwesentlich	**2 geringfügig**	**3 kritisch**	**4 katastrophal**
	Auswirkung / Schadensausmass				

[7] https://www.beurteilung.apps.be.ch/beurteilung/SetLanguage.do

Beispiele von häufig eintretenden Risiken mit verschiedenen Schutzmassnahmen:

	Szenario/Risiko	Schadens-ausmass	Eintrittswahrscheinlichkeit	Risiko	Schutzmassnahmen (verschiedene Beispiele aus Sicht der Schule)
2.a	Durchführung von Produkten/Lernkontrollen inklusive Beurteilung (Prädikat/Benotung). Die Prüfungsresultate werden in der Schule publik.	2	3	6	Die Lehrpersonen werden geschult, die einzelne Beurteilung nicht im gleichen Dokument zu vermerken, sondern diese in der entsprechenden Fachapplikation zu dokumentieren.
2.b	Dokumentation prognostische Beurteilungen/Einschätzungen. Würden solche Beurteilungen bekannt, könnte das den Betroffenen nachhaltig schaden, zum Beispiel im Zusammenhang mit der Berufswahl.	3	3	9	Das Konzept der Schule sieht vor, dass diese vertraulichen Daten nur in der spezifischen Fachapplikation bearbeitet werden dürfen. Die Sensibilisierung/Schulung hierzu ist in [(Referenzen anfügen] ausgewiesen. Die Fachapplikation wird mit einer Zwei-Faktor-Authentifizierung betrieben.
7.a	Erstellen von Förderplänen im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen im Regelschulangebot (MR, ehemals IBEM) werden erstellt und in Onedrive gespeichert. Administratoren von Microsoft können auf diese Daten zugreifen. Behördenzugriffe seitens der USA (Cloudact) sind aufgrund von fehlenden Kontrollmöglichkeiten nicht überprüfbar.	3	4	12	Customer Lockbox verhindert einen unautorisierten Zugriff auf solche Daten. Daneben ist eine automatische Funktion eingebaut, die bei einer grösseren Anzahl von Key-Wörtern das Sensitivity-Label selbstständig auf der entsprechenden Stufe aktiviert respektive in diesem Fall mit dem Schlüssel der Schule verschlüsselt. Der Umgang mit dieser Sicherheitsfunktion auf Dokumentenebene wird in definierten Schulungen den Nutzerinnen und Nutzern nähergebracht und erläutert. Lehrpersonen nutzen die Zwei-Faktor-Authentifizierung. Oder: Die Förderpläne werden in einem anderen Textverarbeitungsprogramm als Word auf dem Computer der Lehrperson erstellt und unter Umständen in der spezifischen Fachapplikation gespeichert.
7.b	Diese Förderpläne werden per Mail der Schulleitung oder auch den Erziehungsberechtigten zugestellt. Die Gefahr einer fälschlich eingegebenen Mailadresse ist gross. Der Schaden für die betroffene Person kann unter Umständen gross sein (Mobbing, Cybermobbing).	3	4	12	Entweder: Mailinhalte und Anhänge an externe Mailadressen werden verschlüsselt. Das Passwort wird über einen zweiten Kanal übermittelt. Zusätzlich wird eine digitale Signatur eingesetzt (S/MIME). Oder: Für die Übermittlung dieser Inhalte per Mail wird ein separater Maildienst mit zusätzlicher Verschlüsselung eingesetzt. Beispiel: Protonmail. Dieser Maildienst wird mit einer Zwei-Faktor-Authentifizierung betrieben Oder: Dateien werden nur als Link auf einem dritten, sicheren Server mittels separatem Passwort freigegeben. Beispiel: Proton Drive oder Tresorit / Tresorit Send
8	Die Nutzenden vergessen ihr Passwort. Eine Administratorin/ein Administrator kann jederzeit die Passwörter der Nutzerinnen und Nutzer zurücksetzen und sich potenziell auch Zugang zu den Daten verschaffen. Passwortlisten bergen die Gefahr, dass Konten gehackt werden.	2	3	6	Die Admin-Rolle ist im Rollen- und Berechtigungskonzept verankert. Eine zusätzliche Vereinbarung regelt die Rechte und Pflichten. Die Nutzerinnen und Nutzer erhalten ein Default-Passwort und müssen dieses bei der nächsten Anmeldung erneuern.

4.5 Restrisiken ausweisen

Auch wenn die aufgeführten Massnahmen umgesetzt werden, können Risiken verbleiben (Restrisiken). Zurzeit sind die meisten Restrisiken in fehlenden Kontrollmechanismen auszumachen.
Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

Beispiele
Vertragsgebundene Restrisiken:

- Fehlende Überprüfbarkeit der Zugriffe auf die Daten durch Microsoft bzw. Subunternehmen von Microsoft.
- Fehlende Überprüfbarkeit der Zugriffe durch amerikanische Sicherheitsbehörden (Cloud Act)
- Die verantwortliche Behörde kann nicht überprüfen, ob Personendaten, die für eine Zwei-Faktor-Authentifizierung verwendet werden (Name, Vorname, Geschäftliche Mail, unter Umständen private Handynummer) auch wirklich nach der vertraglich festgelegten Dauer der Speicherung unwiderruflich gelöscht werden.
- Auch im Rahmenvertrag von Educa vertraglich legitimierte Bekanntgabe von Telemetrie-Daten an US-amerikanische Subunternehmen.
- Erfassung der Nutzenden mit Vor- und Nachnamen. Diese Personendaten bergen das Risiko des Profilings.
- Einseitige Vertragsanpassungen durch Microsoft.

Schulorganisatorische Restrisiken:

- Die Passwörter von Schülerinnen und Schülern im Zyklus 1 werden durch die verantwortliche Lehrperson der Klasse verwaltet
- Rückmeldungen zu Arbeiten von Schülerinnen und Schülern im selben Dokument können als formative Beurteilung interpretiert werden.

4.6 Verschlüsselung

Bei der Nutzung von Microsoft 365 ist die Übertragung und die Speicherung der Daten standardmässig verschlüsselt («data in transit» und «data at rest»). Microsoft verfügt über den entsprechenden Schlüssel und kann damit grundsätzlich auf die in der Cloud verschlüsselt hinterlegten Daten zugreifen. Während des eigentlichen Bearbeitungsvorganges der Daten in der Cloud («data in process») sind diese nicht verschlüsselt.
Das Risiko der unbefugten Dateneinsicht durch Mitarbeitende von Microsoft (bzw. von Mitarbeitenden entsprechender Subunternehmen) kann grundsätzlich durch die Aktivierung des Customer-Lockbox-Prozesses oder durch die Verwendung eines eigenen behördenseitigen Schlüssels (zum Beispiel bei der Bearbeitung von vertraulichen Daten) minimiert werden.
Der Customer-Lockbox-Prozess kann über den A5-Plan von Microsoft aktiviert werden. Microsoft verpflichtet sich damit vertraglich, den Schlüssel nur mit der ausdrücklichen Zustimmung der Behörde zu verwenden. Die verantwortliche Person der Schule, die die entsprechende Zustimmung erteilen darf, muss im Rollen- und Berechtigungskonzept festgehalten werden.
Damit ist aber immer noch nicht ausgeschlossen, dass US-Behörden via Cloud Act Zugriff auf gespeicherte Daten haben können.
Hier bietet Microsoft die Möglichkeit, auch einen eigenen Schlüssel der Behörde (Schule/Gemeinde) zu verwenden (sog. «Hold Your Own Key»). Die Umsetzung dieser Massnahme ist technisch anspruchsvoll.

Bei einem Einsatz von Outlook in Zusammenhang mit vertraulichen Daten ist darauf zu achten, dass der S/MIME-Standard für das Signieren von Mails implementiert ist. S/MIME ist in der Risikobeurteilung zu berücksichtigen. Aufgrund der zahlreichen externen Mail-Kontakte einer Schule greift die Verschlüsselung von S/MIME nur in spezifischen Anwendungsszenarien.

Weiter sind auf dem Markt Lösungen für Datenspeicherung oder für Mail mit stärksten Sicherheitstechnologien verfügbar. Wichtig hierzu sind Abklärungen, ob es sich um eine Firma mit Gerichtsstand Schweiz und Serverstandort Europäische Union/Schweiz handelt und wie sich die Benutzerfreundlichkeit im Schulumfeld gestaltet. Beispiele sind dem Navigator von educa zu entnehmen.

4.7 Protokollierung

Bei der Nutzung von Microsoft 365 können Daten über die Nutzenden und deren Aktivitäten automatisch erfasst und gespeichert werden (Log-Daten).

Eine Auswertung dieser Log-Daten darf aber nur unter bestimmten Voraussetzungen getätigt werden (vgl. hierzu die kantonale Randdatenverordnung RDV):

- Bei technischen Problemen
- Bei Missbrauchsverdacht:
    - Eine hinreichende schriftliche Begründung des konkreten Missbrauchsverdachts oder
    - Ein erwiesener Missbrauch.
    - Eine schriftliche Information der betroffenen Person

Die automatisierte Übermittlung von Diagnosedaten an Microsoft ist zu unterbinden (Vgl. 4.14 Diagnosedaten).

4.8 Authentifizierung und Passwörter

Für Administratorinnen und Administratoren ist eine Zwei-Faktor-Authentifizierung notwendig. Diese kann in Microsoft 365 aktiviert werden und ist kostenlos.
Für Lehrpersonen wird die Zwei-Faktoren-Authentifizierung empfohlen. Der Verzicht auf eine Zwei-Faktoren-Authentifizierung (Anmeldung mit einem einzigen Single-Faktor) birgt ein hohes Risiko, da damit eine unrechtmässige Übernahme des Kontos durch eine andere Person ermöglicht wird.

Microsoft 365 bietet grundsätzlich drei Arten der Authentifizierung:

- Verwendung der integrierten Microsoft 365-Authentifizierung
- Synchronisation des Passworts aus dem internen Active Directory zu Microsoft 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 Zweck und Umfang der Datenbearbeitung sowie die Art der bearbeiteten Daten zu berücksichtigen.

4.9 Rollen- und Berechtigungen

Die erteilten Rollen- und Berechtigungen sind jährlich zu prüfen. Jede Person soll nur auf diejenigen Daten zugreifen können, die sie auch tatsächlich benötigt.

4.10 Erfassen der Nutzerinnen und Nutzer

Microsoft bearbeitet nicht nur die innerhalb der Cloud-Dienste übermittelten Personendaten (also insbesondere Inhaltsdaten), sondern auch von den Nutzerinnen und Nutzer selbst bzw. von ihren Diensten

generierte Daten über die Nutzerinnen und Nutzer (zum Beispiel Rand-, Telemetrie- oder Protokollierungsdaten). Diese zusätzlichen Personendaten sind mit der gleichen Sorgfalt zu behandeln wie die Daten, die zur eigentlichen Aufgabenerfüllung bearbeitet werden.

Folglich ist auch bei der Erfassung der Nutzerinnen und Nutzer darauf zu achten, dass nur die nötigsten Angaben erfasst werden (Datensparsamkeit).
Sollten die Daten explizit in der Cloudversion erfasst werden, so sind ausser der Namen keine weiteren Attribute zu erfassen.
Bei Bedenken oder auf Wunsch soll eine Pseudonymisierung angeboten werden.

4.11 Synchronisation von Nutzerdaten

Verschiedene Szenarien verlangen eine Synchronisation der Nutzerdaten mit der Cloud von Microsoft (auch US-amerikanische Server). Beispielsweise sind dies:

- Passwort-Reset-Dienst (SPR)
- Zwei-Faktor-Authenthifizierung
- Aktivierung von Lizenzen

Nur zwingend nötige Nutzerdaten sollen übermittelt werden.
Auch bei einem Einsatz eines Identitätsproviders (IdP) sollen nur zwingend nötige Attribute übermittelt werden. Beispiel: Der Einsatz eines Azure-Active-Directory als IdP für die Anbindung an edulog.

4.12 Löschen

Das Löschen der Daten kann analog physischer Daten betrachtet werden. Es gelten die Aufbewahrungspflichten des Kantons Bern. Daten, die nicht mehr benötigt werden, müssen gelöscht werden. Die Nutzerinnen und Nutzer sollen die Möglichkeit erhalten, ihre Daten vor der Löschung auf ein anderes Speichermedium zu transferieren.

Die Löschung der Protokolldaten erfolgt automatisiert. Die Speicherfristen können unter folgendem Link eingesehen werden: https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview .

4.13 Datensicherung und Notfallplanung

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

4.14 Diagnosedaten

Wird Microsoft 365 Pro Plus lokal auf dem Computer oder die mobile Version (für Tablets oder Smartphones) von Microsoft 365 eingesetzt, werden je nach gewählter Option Daten an Microsoft übermittelt. Deshalb sind von den Administratorinnen und Administratoren entsprechende Massnahmen zu treffen.

Dies bedeutet insbesondere, dass:

- stets die aktuellen Versionen zu verwenden sind
- bei den Diagnosedaten die Option «Weder noch» zu aktivieren ist

- die «optional verbundenen Erfahrungen» zu konfigurieren und nach Möglichkeit zentral zu deaktivieren sind
- die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit zu deaktivieren ist (Microsoft Customer Experience Improvement Program, CEIP)

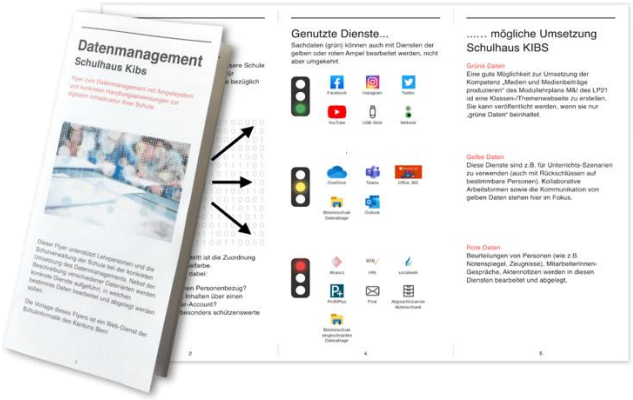
5 Informationen der betroffenen Personen

Nutzerinnen und Nutzer sind über den geplanten Einsatz von Microsoft 365 in der Schule im Vorfeld zu informieren. Dabei sind die wichtigsten Risiken und die getroffenen Schutzmassnahmen offenzulegen.

Die Nutzerinnen und Nutzer erhalten eine Zusammenstellung, welche Dienste von Microsoft 365 in der Schule genutzt und wie sie eingesetzt werden.

Die Schulinformatik der PHBern bietet hierzu einen für jede Schule konfigurierbaren Ampelflyer an[8].

Beispiel eines Ampelflyers:



5.1 Schulung und Sensibilisierung

Die Schulungen zur Infrastruktur und die Sensibilisierung in datenschutzrelevanten Anwendungsbereichen soll beginnen, sobald die Infrastruktur implementiert ist und genutzt wird.

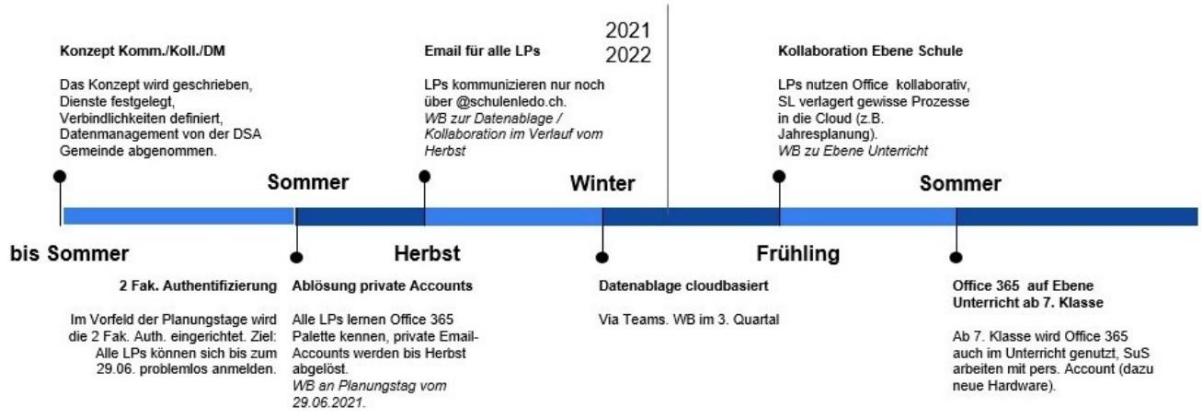
5.1.1 Lehrpersonen

Die Weisungen zum Umgang mit Daten in der Schule ergänzen die technischen Schutzmassnahmen (Vgl. 4.4 *Beispiele*).
Schulen sind mit starken Fluktuationen im Lehrpersonalbereich konfrontiert. Hier gilt es sicherzustellen, dass *neue* Lehrpersonen unkompliziert und schnell die wichtigsten Informationen zur Nutzung der Schulhausinfrastruktur erhalten.
Auch hierzu dient der konfigurierbare Ampelflyer der Schulinformatik der PHBern.

[8] https://kibs.ch/datenschutz

Die Erfahrungen der Schulinformatik der PHBern haben gezeigt, dass eine kontinuierliche Weiterbildung der Lehrpersonen zur Infrastruktur (zum Beispiel durch die Spezialistinnen und Spezialisten Medien und Informatik, SMI) nachhaltiger ist als eine einmalige Schulung durch eine externe Firma.
Zentrale Abläufe zur Handhabung oder auch Sensibilisierungsthemen in multimedialer Form können Lehrpersonen unterstützen und die SMI entlasten.

Beispiel einer Planung zur Einführung von Office 365 über 1 Jahr



5.1.2 Schülerinnen und Schüler

Die Schulung der Schülerinnen und Schüler kann im Konzept Medien und Informatik der Schule unter den Anwendungskompetenzen des Modullehrplans Medien und Informatik geschehen.

6 Eltern

Eltern sollen über den geplanten Einsatz von Microsoft 365 frühzeitig (vor der Implementierung) informiert werden.

6.1 Informationen der Eltern

Die Information der Eltern soll auf mehreren Kanälen erfolgen. Einerseits sollen alle Konzepte zur Infrastruktur und zu Medien und Informatik im Unterricht (Vgl. Empfehlungen[9]) transparent und frei zugänglich sein. Andererseits sollen die Erziehungsberechtigten auch die Möglichkeit erhalten, Fragen zu stellen und Bedenken zu äussern.

6.1.1 Dokumente

- Konzept Medien und Informatik (Konzept aus Empfehlungen des Kantons Bern) [10]– Beispiele für dessen Inhalt:
    - Unterricht und Unterrichtsentwicklung
    - Personalentwicklung
    - Kollaboration und Kommunikation
    - Datenmanagement und Rechtliches
    - Technik und Finanzierung
- Konzept zur Cloud-Infrastruktur / Cloudkonzept (Konzept gefordert aus diesem Merkblatt)

[9] Empfehlungen an die Gemeinden und an die Schulleitungen
[10] Unterstützung bietet kibs.ch, Schulinformatik PHBern

6.1.2 Veranstaltung

Eine an die Eltern gerichtete Veranstaltung – bevor die Infrastruktur implementiert wird –, ist ein wichtiger Bestandteil in der Kommunikation zur Personendatenbearbeitung der Schule/Gemeinde.

Nebst den allgemeinen Informationen zur Infrastruktur soll auch die Unterrichtsebene (Modullehrplan Medien und Informatik) beleuchtet werden. Idealerweise nehmen an dieser Veranstaltung alle Beteiligten der Konzeptarbeiten teil (Gemeinde, kommunale Datenschutzaufsichtsstelle, Schulleitung, SMI, Lehrpersonen, evtl. Firmen und/oder PHBern).
Die Veranstaltung kann so dazu beitragen, dass Bedenken oder Wünsche aufgenommen respektive erfüllt werden.

6.1.3 Kenntnisnahme

Wurde Microsoft 365 gemäss diesem Merkblatt implementiert, kann davon ausgegangen werden, dass die Erziehungsberechtigten die Umsetzung zur Kenntnis genommen haben.

7 Anhänge

7.1 Die wichtigsten Microsoft 365-Dienste unter den Rahmenverträgen (Übersicht).

Quelle: Leitfaden Microsoft 365 im Bildungsbereich, Datenschutzbeauftragte des Kantons Zürich.

Dienst	Beschreibung	Lokale Alternative
Azure Active Directory	Verwaltung oder Abbildung der Identitäten.	
Bookings	Vereinfacht die Planung und Verwaltung von Terminen. Beispiel: Elterngespräche.	
Classroom Tools	Verschiedene schulrelevante Funktionalitäten, Dienste und Apps wie Lerntools, Lesefortschritt und Lesecoach Funktionen, Barrierefreiheits-Checker, Take a Test app, Set up School PCs app.	
Compliance	Verschiedene Dienste und Funktionen wie Rights-Management, Information Protection, Data Loss Prevention, Communication Compliance, Encryption, Customer Lockbox etc.	
Delve	Analysiert und visualisiert die eigene Nutzung und bringt innerhalb von Microsoft 365 für die Nutzenden interessante Dokumente und Informationen an die Oberfläche.	
Exchange, Exchange Online	E-Mail, Kalender, Kontakte, Aufgaben.	X
Flow	Geschäftsprozessautomatisierungstool zum Erstellen von automatisierten Workflows zwischen Apps und Diensten, um Benachrichtigungen zu erhalten, Dateien zu synchronisieren, Daten zu erfassen usw.	
Forms	Formular-Tool Beispiel: Lernkontrolle; zeigt an, was falsch ist.	

Groups	Erlaubt es, Gruppen von Nutzenden zu bilden, mit denen Inhalte aus den verschiedenen Diensten geteilt werden könne.	
Intune und Intune for Education	Zum Einrichten und Verwalten der Geräte.	
Lists	Erstellen, freigeben und nachverfolgen von Listen. Beispiel: Planung Schulfest.	
Microsoft 365 Apps for Enterprise	Installierte Office Anwendungen wie z.B. Word, PowerPoint oder Outlook, welche als Produktivitäts-Apps dienen.	
Minecraft: Education Edition mit Code Builder	Die Education-Version des blockbasierten Spieles ermöglicht Szenarien im Schulumfeld und insbesondere auch das Erlernen des Programmierens.	
Office 365 Plattform mit Office für das web	Hiermit ist die Office 365 Online-Umgebung, also die Cloud-Umgebung der Schule gemeint – der Rahmen, in welchem viele der Dienste, die Tenant-Administration ebenso wie die Web-Versionen der Office-Anwendungen zur Verfügung stehen.	
OneDrive for Business	Persönlicher Dokumentenspeicher für eigene Dokumente.	X
OneNote	Notizprogramm Beispiele: Unterrichtsvorbereitung, elektronische Wandtafel usw.	X
OneNote Kursnotizbuch	Das OneNote-Kursnotizbuch bietet Zusatzfunktionen zu OneNote. Beispiele: Verteilen von Arbeitsblättern an Lernende, vereinfachtes Korrigieren von Hausaufgaben usw.	
Phone System	Kostenpflichtige Ergänzung von Teams für die Teams-Telefonie. Beispiel: Teams-Telefonie für die Schulzimmer, den Hort usw.	
Planner	Teamarbeitstool für Tätigkeiten wie Pläne erstellen, Aufgaben organisieren und zuweisen, Dateien freigeben, Aufgaben im Chat besprechen und sich austauschen.	
PowerApps	Ermöglicht das Erstellen von benutzerdefinierten Business-Apps.	
Power Automate	Workflows zwischen Apps, Daten und Dateien erstellen, um zeitaufwändige Aufgaben zu automatisieren. Beispiel: Beschaffungsantrag einreichen, bewilligen und ablegen.	
PowerBI	Business Intelligence. Zusammenzug von Tools zur Analyse und Visualisierung von Daten, die auf SharePoint gespeichert sind, und zum Teilen der Resultate.	
Project, Project Online	Umfangreiches Projektmanagement-Tool.	X
School Data Sync	School Data Sync ist ein Dienst in Microsoft 365 für Bildungseinrichtungen, der die Schul- und Dienstlisten aus dem Student Information System einer Schule liest. Damit werden Microsoft 365-Gruppen für Exchange Online und SharePoint Online, Klassen Teams für Microsoft Teams und OneNote-Klassen Notizbücher automatisiert erstellt.	

SharePoint, SharePoint Online	Speicherort für Dokumente, die mit anderen Nutzern in vordefinierten Gruppen (siehe «Groups») geteilt werden.	X
Sicherheit	Verschiedene Dienste und Funktionen zur Sicherung der Daten und der Umgebung wie z.B. Microsoft Defender for Office 365, for Cloud Apps, for Endpoint, Antivirus, Advanced Threat Analytics etc.	
Skype for Business	Chatten, Telefonie, Videokonferenzen, Teilen des Bildschirms und von Anwendungen usw. Telefongespräch wird nicht gespeichert, nur Chat (auf dem Exchange Server). Videogespräche können aufgenommen und auf SharePoint gespeichert werden.	(X)
Stream	Schulinterne Videoplattform: Videos speichern, durchsuchen, teilen.	
Teams und Classroom experiences in Microsoft Teams	Chat-basierte Arbeitsumgebung in Microsoft 365. Zusammenzug von Microsoft 365-Diensten, mit starkem Fokus auf Teaminteraktion. Beispiel: Kombination von Skype, SharePoint und OneNote.	
To-Do	To-Do ist in Microsoft 365 integriert und hilft bei der Aufgabenverwaltung, beim Organisieren des Tagesablaufs.	
Visio	Komplexe Informationen visuell vereinfachen und vermitteln. Beispiel: Organigramme, Diagramme.	
Viva Connections	Viva Connections ist eine sharepoint-basierte Plattform für die Schule, welche Kommunikation, Austausch und Vernetzung unterstützt. Beispiel: Intranet, Interne Homepage.	
Viva Insights	Produktivität verbessern.	
Viva Learning	Bietet die Möglichkeit, den Zugang zu Lerninhalten nahtlos in Teams zu integrieren, Kurserfolge nachzuverfolgen, zu teilen etc. (nur für Faculty). Beispiel: Teams-Kurse für Lehrpersonen; Nutzer-Schulungen von Fachanwendungen.	
Whiteboard; Whiteboard in Team	In einem Freihandzeichenbereich gemeinsam Ideen entwickeln und zusammenarbeiten. Beispiel: Gruppenarbeiten, Brainstorming.	

7.2 Andere Dienste unter den Rahmenverträgen (Auszug)

Dienst	Beschreibung
Azure Cloud Plattform	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.
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.
EMS E3 for 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.
Intune	Verwaltung von Apps und Geräten.
Intune for Education	Intune for Education bietet gegenüber Intune eine vereinfachte Nutzungsoberfläche. Es kann eigenständig oder im Zusammenspiel mit der in Intune verfügbaren vollständigen Umgebung zur Geräteverwaltung genutzt werden.
Infrastruktur und Server	Produktivitäts-Server wie Exchange, SharePoint, SQL etc etc.

7.3 Von den Rahmenverträgen nicht abgedeckte Dienste

Die folgenden Dienste können nicht datenschutzkonform genutzt werden. Unter anderem speichern sie Daten ganz oder teilweise ausserhalb der EU.

Dienst	**Beschreibung**
OneDrive (Consumer Version)	Dokumentenspeicher für private Dokumente Schulen können für einen datenschutzkonforme Dokumentenspeicher nur OneDrive for Business einsetzen (siehe Ziffer 9.1).
Skype (Consumer Version)	Kommunikation: Chatten, Telefonie, Teilen des Bildschirms usw. Schulen können als datenschutzkonformes Kommunikations-Tool nur Teams oder Skype for Business einsetzen (siehe Ziffer 9.1).
Sway	Online-Präsentationserstellungstool, das wie eine Website funktioniert.
Yammer	Social Media für Unternehmen.