Muster Datenschutzfolgeabschätzung

für den Einsatz der Lern- und Kommunikationsplattform Microsoft 365 an unserer Schule

Schule: [**Bitte angeben**]

Adresse(n): [**Bitte angeben**]

Schulleitung: [**Bitte angeben**]

1. Grundlegende Informationen

Die DSGVO sieht in Art. 35 (3) eine Datenschutzfolgeabschätzung vor, wenn Daten von schutzbedürftigen Personen und vertrauliche Daten verarbeitet werden. Da in unserer Schule teilweise Kinder unter 16 Jahre unterrichtet werden, kann man die Voraussetzungen als erfüllt sehen.

[bitte auswählen und anpassen]

[Variante 1] Das digitale Netzwerk der Schule ist unterteilt in ein Netz für die Verwaltung der Schule und in ein Schulnetz für unterrichtsbezogene Kommunikation. Microsoft 365 wird nur für das Schulnetz eingesetzt. Verwaltungsdaten, die z. B. personenbezogene Daten der Mitarbeiter betreffen, organisatorische Maßnahmen der Schule, gravierende Vorfälle in der Schule wie z. B. Straftaten, werden erstens nicht automatisiert und zweitens nicht über das Schulnetz kommuniziert und werden daher hier nicht betrachtet.

[Variante 2] Sensible Verwaltungsdaten, organisatorische Maßnahmen der Schule, gravierende Vorfälle in der Schule wie z. B. Straftaten, werden nicht elektronisch kommuniziert, sondern ausschließlich in Schriftform und werden daher hier nicht betrachtet.

Eine Datenschutzfolgeabschätzung ist eine Risikoabschätzung. Dabei gibt es Risiken, die der eingesetzten IT-Plattform inhärent sind und solche, die nutzungsabhängig sind und durch geeignete Konfiguration beeinflusst werden können. Wir betrachten diese beiden Aspekte getrennt.

2. Zweck und Art des Einsatzes elektronischer Medien in der Schule [ggf. anpassen]

- Vermittlung von Medienkompetenz laut Schulordnung.
- Ergänzung und Vertiefung der Unterrichtsinhalte durch vorhandene oder von Lehrern aufbereitete elektronische Angebote
- Schrittweise Erarbeitung von Übungsaufgaben und Projekte über einen längeren Zeitraum mittels elektronischer Medien (Datenspeicherung und -austausch)
- Bildung von Lerngruppen mit Datenaustausch und Chat
- Ergänzender Förderunterricht mittels elektronischer Medien
- Logopädischer Sprachunterricht mittels elektronischer Medien (Aussprache, flüssige Rede)
- Distanzunterricht mit Datenaustausch und Audio- und Videounterstützung, falls zur Aufrechthaltung des Unterrichts geboten

3. Detaillierte Verarbeitungszwecke für die Benutzergruppen [ggf. anpassen]

1. Schüler

a) Bereitstellung von verpflichtenden und fakultativen Übungsaufgaben, Projektaufgaben und Hausaufgaben durch Klassenlehrer im Datenspeicher der Lernplattform, auf den alle Schüler einer Klasse Zugriff haben
b) Bereitstellung von verpflichtenden und fakultativen Übungsaufgaben, Projektaufgaben und Hausaufgaben durch Klassenlehrer im Datenspeicher der Lernplattform, auf den nur der betreffende Schüler und Lehrer Zugriff haben
c) Rückgabe der bewältigten Übungsaufgaben und Hausaufgaben durch Schüler im Datenspeicher der Lernplattform, auf den nur der betreffende Schüler und Lehrer Zugriff haben
d) Elektronische Kommunikation zwischen Lehrer und Schüler betreffend Abgabetermine, allgemeine Fragen zu Hausaufgaben
e) Einsatz von Audio- und Video-Plattform für logopädisch unterstütztes Sprachlernen. Schüler erhalten Audio-Übungsaufgaben und reichen sie ein.
f) Distanzunterricht: Einsatz von Audio- und Video-Plattform mit Einsatz des Datenspeichers der Lernplattform
g) Distanzunterricht: Mitteilung der Bewertung von Übungsaufgaben, Projektaufgaben und Hausaufgaben durch Klassenlehrer per elektronischer und/oder Audio- oder Video-Kommunikation

2. Lehrkräfte und Schul-Verwaltung
   a) Bereitstellung von Unterlagen und Terminen für schulische Veranstaltungen, Diskussion von Lehrinhalten, Lehrplänen
   b) Elektronische Kommunikation zu dienstlichen Aufgaben einzelner oder mehrerer Lehrkräfte, Vertretungen, Ausfallsplanung
3. Eltern
   a) Mitteilung zu wichtigen schulischen Angelegenheiten: Hausaufgaben, Fehlzeiten, Abholung, Konflikte
4. Dienstleister, Systembetreuer
   a) Kontenverwaltung, Sicherheitseinstellungen, Aktualisierungen, Behebung technischer Probleme

4. Rechtsgrundlage für Datenverarbeitung

- Die rechtliche Grundlage für den Einsatz einer IT-Plattform an einer öffentlichen oder privaten Schule, die öffentlich akkreditiert ist, ist Art. 6 Abs.1 lit c und e DSGVO in Verbindung mit dem Paragraphen [**bitte ergänzen**] über die Verarbeitung personenbezogener Daten aus dem Schulgesetz des Bundeslandes.
- Der Auftragsverarbeitungsvertrag von Microsoft inklusive der aktuellen Standardvertragsklauseln (online verfügbar: Microsoft DPA)
- Der Auftragsverarbeitungsvertrag mit unserem Schulträger/Sachaufwandsträger **[falls zutreffend bitte angeben]**
- Der Auftragsverarbeitungsvertrag mit unserem Dienstleister für Systembetreuung **[falls zutreffend bitte angeben. Dann weiter auf Seite 12]**

5. Eingesetzte Technologien für das Schulnetz

Als technologische Plattform zur Erreichung der im Abschnitt 2 und 3 genannten Zwecke sollen die Anwendungen Exchange Online, Sharepoint Online und Teams, sowie die Desktop-Version von Word, Excel, Powerpoint, OneNote, Outlook (sog. Microsoft 365 Apps for Enterprise) aus der Microsoft 365 Suite eingesetzt werden. Teams ergänzt die ersten beiden aufgeführten durch Audio-, Video-, und Chatfunktionen.

5.1 Teams

Teams ist die Plattform für Zusammenarbeit in Office 365.
Innerhalb von Teams können Teamräume für Projekte eingerichtet werden. Die Teamräume können dann wieder in verschiedene Kanäle unterteilt werden. Innerhalb eines Kanals werden die Funktionen und Apps zusammengestellt, die an dieser Stelle gebraucht werden. Kanäle können moderiert sein, d.h. Beiträge werden vor der Veröffentlichung durch einen Moderator gesichtet und freigegeben.

5.1.1 Chat

Im Rahmen von Teams werden zwei Arten von Chats unterschieden: private Chats und Kanal-Chats (Beiträge).

Private Chats finden außerhalb eines dedizierten Teamraums zwischen zwei oder mehreren Benutzern statt. Nur die direkten Teilnehmer eines Chats haben Zugriff auf seinen Inhalt. Sie können Ende-zu-Ende verschlüsselt werden. Kanal-Chats (oder auch „Beiträge“) sind Nachrichten innerhalb eines Kanals im Rahmen eines Teamraumes. Alle Mitglieder eines Teamraumes haben lesenden Zugriff auf Kanal-Chats und können auf diese Antworten.

Beide Arten von Chat-Nachrichten sind in Teams standardmäßig persistent, werden also nicht nach einem bestimmten Zeitraum gelöscht. Über „Nachrichten-Richtlinien“ kann festgelegt werden, wer Chat-Nachrichten löschen kann: der Besitzer eines Teams, der Verfasser der Nachricht, oder beide.

Über Aufbewahrungs-Richtlinien (Retention Policies) können Regeln definiert werden, mit denen Chat-Nachrichten nach einem bestimmten Zeitraum automatisch gelöscht werden. Hier kann zwischen privaten Chat-Nachrichten und Kanal-Chats unterschieden werden.

5.1.2 Apps

Der Funktionsumfang von Teams kann durch Apps erweitert werden. Administrativ kann festgelegt werden, ob dieser App-Store den Benutzern überhaupt zur Verfügung stehen soll und wenn ja, welche Apps enthalten sein sollen. An unserer Schule wird als einzige App das eingebaute Klassennotizbuch verwendet.

5.1.3 Audio-Video Funktionen

Teams verfügt über Funktionen für Audio- und Videokonferenzen zwischen bis zu 20.000 Teilnehmern. Im Rahmen einer Besprechung (Konferenz / Meeting) können Bildschirminhalte für alle Teilnehmer freigegeben werden. Audio- und Videokonferenzen können aufgezeichnet werden, sofern entsprechende Lizenzen dafür gekauft wurden. Wird eine Aufzeichnung gestartet, so wird jeder Teilnehmer automatisch auf diesen Umstand hingewiesen. Die Speicherung der Aufzeichnung erfolgt im persönlichen Datenspeicher OneDrive des Vortragenden. Eine Freigabe für die Teilnehmer ist wahlweise möglich.

5.1.4 Klassennotizbuch

Das Klassennotizbuch basiert auf dem Office Programm OneNote und ist eine Art digitales Schulheft. Die Lehrkraft kann Übungsmaterial und Aufgaben selektiv in die einzelnen Notizbücher der Schüler verteilen oder Übungen zentral für alle lesbar und/oder auch schreibbar bereitstellen, sie kann die Aufgaben digital einsammeln, bewerten und den Schülern individuell Rückmeldung geben.

5.2 Sharepoint

SharePoint stellt im Zusammenhang mit dem Einsatz von Teams in der Schule den Datenspeicher dar und dient zur Ablage und Bereitstellung von Dokumenten. in SharePoint können mehrere Benutzer gleichzeitig an einem Dokument arbeiten. Außerdem hat SharePoint eine eingebaute Versionshistorie zu jedem Dokument. Standardmäßig haben alle Mitglieder eines bestimmten Teams Lese- und Schreibrechte auf die im Team bereitgestellten Dokumente, dies kann aber auf Leserechte oder kein Zugriff auf bestimmte Dateien beschränkt werden.

5.3 OneDrive for Business

OneDrive for Business ist ein Teil von SharePoint Online, der speziell als persönlicher Speicherort für Dokumente gedacht ist. Im Normalfall hat nur der Benutzer selbst Zugriff auf sein OneDrive for Business, es können jedoch Dokumente oder Bibliotheken mit anderen geteilt (freigegeben) werden. Alle in OneDrive gespeicherte Daten können im Verlustfall durch die eingebaute Dateihistorie zu einem früheren Stand wieder hergestellt werden.

5.4 Exchange

Die zentrale Aufgabe von Exchange Online ist das Bereitstellen von E-Mail-Funktionen wie E-Mails, Kalender, Kontakte und Aufgaben. Um mit Exchange Online arbeiten zu können, erhält jeder Benutzer ein Postfach. In diesem Postfach werden sämtliche benutzerbezogene Daten gespeichert. Der Zugriff auf das Postfach erfolgt entweder über die Weboberfläche (Outlook im Web) oder durch Outlook für Windows, macOS, iOS oder Android. Exchange enthält Technologien zur Durchsuchung und langfristiger, rechtssicherer Speicherung von Daten, die in der Schule nicht benötigt und nicht eingesetzt werden.

5.5 Azure Active Directory

Das Azure Active Directory (AAD) ist der zentrale Verzeichnisdienst für alle unter dem Begriff „Microsoft 365“ zusammengefassten Dienste. Es ermöglicht einmal die Authentifizierung des Benutzers durch Benutzername, Passwort und einem weiteren Faktor (sog. Mehr-Faktor-Anmeldung) und die Autorisierung für die dem Benutzer zugewiesenen Rechte und Aufgaben. Ohne ein Konto im AAD ist die Nutzung der Microsoft 365 Dienste nicht möglich.

5.5.1 Benutzerattribute

Jedem Benutzer können eine Vielzahl von Benutzerattributen zugewiesen werden. Davon werden in unserer Schule nur folgende genutzt: Identität: Vorname und Nachname oder Pseudonym und die automatisch erzeugte System-ID; Auftragsinformation: Lehrer oder Schüler, Klasse des Schülers, Anmeldung möglich oder blockiert; Zugewiesene Lizenzen (Office, E-Mail, Teams oder nur ein Teil davon).

5.5.2 Rollen und Gruppen

Hier unterscheidet man im AAD generell zwischen „Benutzer“ und „Administrator“. Jedes Benutzerobjekt im AAD gehört zur Rolle Benutzer, es sei denn, ihm wurde eine administrative Rolle zugewiesen. Um die Vergabe von Zugriffsberechtigungen zu vereinfachen, können Benutzer zu Gruppen zusammengefasst werden.

5.5.3 Protokollierung

Um einen störungsfreien und nachvollziehbaren Betrieb gewährleisten zu können, werden alle Aktionen von oder an Objekten im AAD protokolliert. Die protokollierten Informationen können über verschiedene Berichte abgerufen werden, die Metadaten enthalten wie Zahl und Größe der von Benutzern angelegten Objekte. Diese Daten sind standardmäßig anonymisiert und können nur von Administratoren abgerufen werden.

Man kann unterscheiden zwischen den Überwachungsprotokollen, in denen jegliche administrativen Aktivitäten in Microsoft 365 festgehalten werden wie Anlage oder Löschung von Benutzerkonten und Sicherheitsprotokollen. Letztere bieten eine Übersicht über legitime oder sog. „riskante" Anmeldungen an das System, die auf Kompromittierungen hinweisen.

6. Nutzungskonzept

Jeder Schüler und jeder Lehrer erhält ein persönliches Konto mit Datenspeicher, Chatfunktion, ggf. Audio- und Videofunktion

6.1 Berechtigungskonzept

Jeder Lehrer kann seinen Schülern Daten zur Verfügung stellen und je nach Funktionsumfang der Plattform chatten und/oder per Audio- und Video mit seinen Schülern kommunizieren. Jeder Schüler kann mit anderen Schülern einer Klasse Daten austauschen und ggf. chatten.

6.2 Administrationskonzept

Die von der Schulleitung bestellten Systembetreuer erhalten Administratorrechte zur Verwaltung und zur Problembehebung der elektronischen Medien.

Zusätzlich wird die Schule durch Dienstleister unterstützt, mit denen ein Auftragsverarbeitungs-vertrag besteht.

6.3 Löschkonzept

Verlässt ein Lehrer bzw. Schüler dauerhaft die Schule, werden dessen Daten und Konten nach 3 Monaten bzw. 30 Tagen gelöscht. Bei einer vorübergehenden Unterbrechung des Schuldiensts bzw. Schulbesuchs (z. B. Elternzeit, Auslandsaufenthalt) werden individuelle Vereinbarungen bzw. der Löschung oder Stilllegung elektronischer Dienste getroffen.

7. Gewährleistungsziele (Standard-Datenschutzmodell)

Die vorliegende Datenschutz-Folgeabschätzung orientiert sich zur Beurteilung der Risiken am „Standard-Datenschutzmodell" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder.

Verfügbarkeit/Skalierbarkeit/ Barrierefreiheit	Steht die Lösung nicht wie geplant für die erforderliche Zahl der Nutzer zur Verfügung, kann das verfolgte Lernziel nicht erreicht werden. Ist die Lösung nicht barrierefrei, werden betroffene Personen von der Nutzung ausgeschlossen und damit diskriminiert.
Integrität	Ist ein Zugang zu IT-Systemen leicht zu kompromittieren, leidet die Richtigkeit und Nachweisbarkeit der Daten.
Vertraulichkeit	Eine Lösung mit mangelhaftem Zugangsschutz oder fehlender Verschlüsselung ermöglicht unbefugte Nutzung und damit umfangreiche Missbrauchspotentiale.

Transparenz	Sind Nutzer nicht in der Lage, die Funktionen der Software einzuschätzen, sind Fehlbedienungen und unsachgemäße Nutzung möglich.
Nichtverkettbarkeit	Die automatische Weitergabe oder Übernahme von Daten aus einer Anwendung an eine andere kann den Schaden bei einem Angriff erhöhen.
Intervenierbarkeit	Zur Umsetzung der Betroffenenrechte müssen ein IT-System den Verantwortlichen jederzeit ermöglichen, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen, um den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung usw. zu gewähren.
Datenminimierung	Überflüssige Aufzeichnungen von Konferenzen, Speicherung unnötiger Schülerdaten, fehlende Speicherfrist erhöht das Risiko von Missbrauch.

8. Risikobewertung

Die Bewertung eines Risikos wird unter Berücksichtigung der getroffenen Maßnahmen unterteilt in „Eintrittswahrscheinlichkeit“ und „Auswirkungen“.

Die Einteilung folgt dabei den Vorschlägen dem „Bitkom-Leitfaden für Risk Assessment & Datenschutz-Folgenabschätzung“[1].

Eintrittswahrscheinlichkeit

1) **Vernachlässigbar**: für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist).
2) **Eingeschränkt**: für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist).
3) **Signifikant**: für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat).
4) **Maximal**: für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einer öffentlich zugänglichen Lobby).

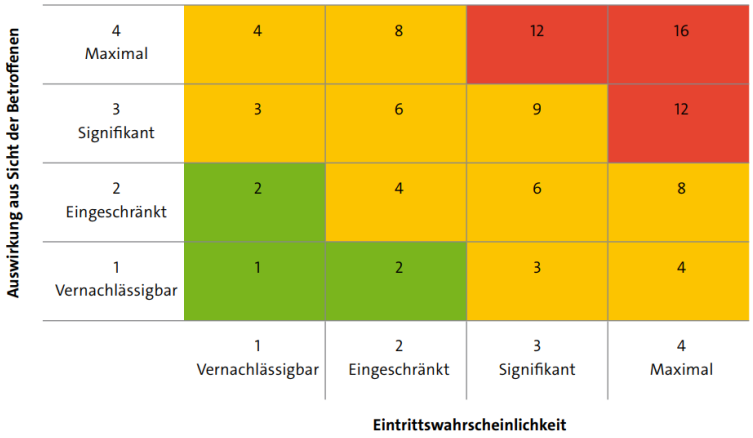
Auswirkungen

1) **Vernachlässigbar**: Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
2) **Eingeschränkt** Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
3) **Signifikant** Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.

[1] https://www.bitkom.org/sites/default/files/file/import/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf

1) **Maximal** Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Das Produkt aus Eintrittswahrscheinlichkeit und Auswirkung wird in Form einer Grafik dargestellt, der sog. Risikomatrix.



9. Risiken

Bei der Nutzung einer digitalen Plattform gibt es 2 Kategorien von Risiken, nämlich systeminhärente und solche, die durch die Nutzung der Plattform entstehen. Eine Plattform, die systeminhärent z. B. die Integrität der Daten nicht garantieren kann, kann nicht risikoarm betrieben werden.

9.1 Evaluierung der systeminheränten Risiken von Microsoft Teams, Sharepoint und Exchange Online

Wir geben erst das Risiko an, dann die Maßnahmen, die die Plattform selbst bietet, um diese Risiken zu minimieren, und schließlich die Eintrittswahrscheinlichkeit, also das verbleibende Risiko, sofern die seitens der Plattform angebotenen Maßnahmen auch genutzt/eingesetzt/implementiert werden.

9.1.1 Risiko fehlende Verfügbarkeit/Skalierbarkeit/ Barrierefreiheit

Bedeutung	Steht die Plattform für die erforderliche Zahl von Nutzern zur Verfügung, sodass das verfolgte Lernziel robust und zuverlässig erreicht werden kann und somit diskriminierungsfreie Teilhabe garantíert ist?
Microsoft 365	Teams steht je nach Lizenz zwischen 300 bis 10000 Benutzern gleichzeitig zur Verfügung. Die Verfügbarkeit wird zu 99,9% gewährleistet (https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services) Alle Office Produkte bieten die Read-Aloud-Funktion, Live-Captions (Speech-to Text) und die Vergrößerung von Texten, automatische Übersetzungen und Unterlegen von Texten mit Bildern (immersive Reader). Damit wird das zukünftige Barrierefreiheitsstärkungsgesetz weit übererfüllt.
Schwere der Auswirkung	Eingeschränkt
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	2

Bedeutung	Bietet das System feste Patch-Zyklen und Support?
Microsoft 365	Ja (https://learn.microsoft.com/en-us/deployoffice/overview-update-channels). Für Microsoft 365 Mandanten mit akademischen Lizenzen ist der technische Support kostenlos verfügbar. Lizenzen für DSGVO konforme Support-Einschränkungen (sog. Lock-Box) sind verfügbar.
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	3

Bedeutung	Können irrtümlich oder bösartig gelöschte Daten zu jedem Zeitpunkt wiederhergestellt werden?
Microsoft 365	Ja. Alle Daten in OneDrive und Sharepoint sind innerhalb der hinterlegten Löschungsfrist vollständig wiederherstellbar. https://learn.microsoft.com/de-de/sharepoint/administration/backup-and-recovery-overview
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Eingeschränkt
Risikofaktor	6

9.1.2 Risiko fehlende Integrität

Bedeutung	Unterstützt die Plattform Ende-zu-Ende-Verschlüsselung der gespeicherten Daten?
Microsoft 365	Ja, https://docs.microsoft.com/de-de/microsoftteams/teams-end-to-end-encryption und https://docs.microsoft.com/de-de/microsoft-365/compliance/information-protection?view=o365-worldwide
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	3

Bedeutung	Werden Daten beim Transfer vom Anwender zu den Servern verschlüsselt?
Microsoft 365	Ja, https://techcommunity.microsoft.com/t5/microsoft-365-blog/how-microsoft-365-encryption-helps-safeguard-data-and-maintain/ba-p/2461066
Schwere der Auswirkung	Eingeschränkt
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	2

Bedeutung	Unterstützt das System eine aktive Warnung vor Schadware?
Microsoft 365	Ja, https://docs.microsoft.com/de-de/power-platform/admin/wp-data-loss-prevention, https://docs.microsoft.com/de-de/compliance/assurance/assurance-malware-and-ransomware-protection, https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/configure-anti-malware-policies?view=o365-worldwide, https://docs.microsoft.com/de-de/microsoft-

	365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide
Schwere der Auswirkung	Maximal
Eintrittswahrscheinlichkeit	Eingeschränkt
Risikofaktor	8

Bedeutung	Erfüllt der Serverbetrieb die Anforderungen aus dem BSI-Grundschutz und sind die gespeicherten Daten serverseitig („at rest“) verschlüsselt?
Microsoft 365	Ja, ISO 20000-1:2011, ISO 27018, BSI C5 und weitere (https://docs.microsoft.com/de-de/compliance/regulatory/offering-home) , alle Daten sind serverseitig verschlüsselt (https://techcommunity.microsoft.com/t5/microsoft-365-blog/how-microsoft-365-encryption-helps-safeguard-data-and-maintain/ba-p/2461066)
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Eingeschränkt
Risikofaktor	6

9.1.3 Risiko fehlende Vertraulichkeit

Bedeutung	Wird Anmeldung an das System mit einem zweiten Faktor (Mehr-Faktor-Anmeldung) unterstützt, um Identitätsdiebstahl zu verhindern?
Microsoft 365	Ja, https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-licensing , es werden biometrische Verfahren, Verfahren mit TOTP Token, Fido2 Schlüssel, Authentikator App, SMS, Telefon, separates E-Mail-Konto, zertifikatsbasierte Anmeldung unterstützt.
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	3

Bedeutung	Ist die Verwendung unsicherer Passwörter systemseitig ausgeschlossen?
Microsoft 365	Ja, alle Passwörter müssen mindestens 8 Zeichen haben und eine gewisse Komplexität aufweisen (https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide). Mit Fido2 Schlüssel oder biometrischen Verfahren (Fingerprint Sensor) sind passwortfreie Anmeldungen möglich
Schwere der Auswirkung	Maximal
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	4

Bedeutung	Können Links oder Anhänge in Chats, E-Mails und Dokumenten automatisch auf Legitimität und Schadfreiheit überprüft werden?
Microsoft 365	Ja, https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/safe-links-about?view=o365-worldwide

Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Eingeschränkt
Risikofaktor	6

9.1.4 Risiko fehlende Transparenz

Bedeutung	Liegt ein Auftragsverarbeitungsvertrag des Anbieters nach Art. 28 DSGVO vor, aus dem unter anderem die technischen und organisatorischen Maßnahmen zum Schutz der Daten hervorgeht?
Microsoft 365	Ja, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA. Die Bedenken der Datenschutzbehörden sind aktuell (Stand Nov 2022) erschöpfend hier beantwortet: https://news.microsoft.com/de-de/microsoft-erfuellt-und-uebertrifft-europaeische-datenschutzgesetze/
Schwere der Auswirkung	Vernachlässigbar
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	1

Bedeutung	Liegen entsprechende Garantien, wie die EU-Standardvertragsklauseln 2021/914, vor, wenn der Auftragsverarbeiter personenbezogene Daten in Drittländer (z.B. die USA) überträgt?
Microsoft 365	Ja, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA enthält diese Standardvertragsklauseln. Microsoft hat die Anforderungen durch weitere Garantien übererfüllt, siehe https://news.microsoft.com/de-de/microsoft-erfuellt-und-uebertrifft-europaeische-datenschutzgesetze/.
Schwere der Auswirkung	Vernachlässigbar
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	1

Bedeutung	Ermöglicht das System automatische Warnungen bei ungewöhnlichen Datenübertragungen wie z. B. Löschen vieler Daten in kurzer Zeit?
Microsoft 365	Ja, https://docs.microsoft.com/de-DE/microsoft-365/security/office-365-security/protect-against-threats?view=o365-worldwide, https://docs.microsoft.com/de-de/microsoft-365/compliance/purview-compliance?view=o365-worldwide
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Eingeschränkt
Risikofaktor	6

9.1.5 Risiko fehlende Nichtverkettbarkeit

Bedeutung	Ermöglicht das System eine automatische Warnung bei unbefugter Weitergabe sensibler Daten, wie z. B. durch Verhinderung der automatischen Weiterleitung an private E-Mailadressen?

Microsoft 365	Ja, https://docs.microsoft.com/de-de/defender-cloud-apps/, spezifisch „Cloud App Discovery“, automatische E-Mail-Richtlinien zur Abwehr von Bedrohungen und Verhinderung von Datenverlust https://docs.microsoft.com/de-de/microsoft-365/compliance/purview-compliance?view=o365-worldwide
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	3

9.1.6 Risiko fehlende Intervenierbarkeit

Bedeutung	Bietet das System die Möglichkeit, alle gespeicherten persönlichen Daten eines Benutzers jederzeit zu extrahieren?
Microsoft 365	Ja, mit https://www.microsoft.com/de-de/security/business/microsoft-priva können Auskunftsersuchen rasch und in großer Zahl erfüllt werden.
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	3

9.1.7 Risiko fehlende Datenminimierung

Bedeutung	Bietet das System die Möglichkeit, die Aufbewahrungszeit von eigenen Daten, Diagnosedaten und Metadaten zu begrenzen und automatisierte Löschungen zu überwachen und durchzuführen?
Microsoft 365	Ja, https://news.microsoft.com/de-de/datenschutz-microsoft/, https://www.microsoft.com/de-de/trust-center/privacy/gdpr-overview, https://learn.microsoft.com/de-de/compliance/regulatory/gdpr-action-plan
Schwere der Auswirkung	Signifikant
Eintrittswahrscheinlichkeit	Vernachlässigbar
Risikofaktor	3

9.1.8 Fazit Systeminhärente Risiken

Es ergeben sich **keine** hohen systeminheränten Risiken.

9.2 Evaluierung der Risiken durch den praktischen Einsatz von Teams, Sharepoint und Exchange Online durch Verfahrensbeteiligte

9.2.1 Risikoquellen

Risikoquellen	**Risiko für Benutzer**	**Eintritts-wahrscheinlichkeit**
Schulleitung	Auswahl der Lernplattform nicht diskriminierungsfrei, nicht sicher nach Stand der Technik, überflüssiger Einbezug oder Nutzung personenbezogener Daten	Vernachlässigbar

Systembetreuer, Dienstleister	Identitätsdiebstahl, Datenverlust, Datenveränderung, Kontrollverlust von persönlichen Daten, Weitergabe persönlicher Daten an Dritte	Eingeschränkt
Andere Benutzer aus der gleichen Schule	Mobbing, Rufschädigung, Identitätsdiebstahl, Datenveränderung, Datenverlust	Eingeschränkt
Externe, Hacker	Identitätsdiebstahl, Kontrollverlust, Datendiebstahl, Erpressung, Drohung, finanzielle Verluste	Signifikant

9.2.2 Risiken

Betrachtet werden die Risiken, die durch die Verarbeitung personenbezogener Daten im Rahmen der Nutzung von Microsoft Teams, Sharepoint und Exchange Online für die Betroffenen entstehen können. Dies können sein:

1. Identitätsdiebstahl
2. Datendiebstahl
3. Unberechtigte Leistungs- und/oder Verhaltenskontrolle
4. Systematische Überwachung
5. Offenlegung vertraulicher oder persönlicher Daten

Den erkannten Risiken werden technische und organisatorische Maßnahmen entgegengesetzt. Diese Maßnahmen dienen entweder dazu, die Eintrittswahrscheinlichkeit eines Risikos zu reduzieren, oder die Schwere der Auswirkungen zu reduzieren.

[Bitte beachten Sie, dass Sie die hier angeführten Maßnahmen auch in der Schule umsetzen müssen. Wenn das nicht möglich ist, müssen Sie das verbleibende Risiko erhöhen. Wenn das Risiko hoch bleibt, dürfen Sie den Dienst nicht einsetzen.]

9.2.2.1 Risiko Verfügbarkeit/ Skalierbarkeit/ Barrierefreiheit

Bedeutung	Können irrtümlich oder bösartig gelöschte Daten zu jedem Zeitpunkt wiederhergestellt werden?			
Microsoft 365	Die Aufbewahrungsfrist für OneDrive bzw. Sharepoint-Daten wurde auf dem Standardwert von 30 Tagen bzw. 93 Tagen belassen. Damit können OneDrive Daten bis zu 30 Tagen zurückgesetzt werden. Alle Sharepoint Daten sind faktisch unbegrenzt versioniert und haben 2 Löschebenen (die zweite zur Wiederherstellung durch den Administrator).			
Schwere der Auswirkung	Signifikant			
Eintrittswahrscheinlichkeit	Schulleitung	Sysadmin	Nutzer	Externe
	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar	Eingeschränkt
Risikofaktor	3	3	3	6

9.2.2.2 Risiko Integrität

Bedeutung	Ist Ende-zu-Ende-Verschlüsselung der gespeicherten Daten konfiguriert und für alle Mitarbeiter verfügbar und werden die aktiven Systemwarnungen beachtet?
Microsoft 365	Die Lehrer werden darin geschult, Schülerdaten grundsätzlich Ende-zu-Ende zu verschlüsseln **[dies erfordert gewisse Lizenzen, bitte ggf. anpasssen]**. Die Systemadministratoren kontrollieren regelmäßig mittels der eingebauten Sicherheits-Funktionen, ob riskante Anmeldungen auf Kompromittierung von Benutzerkonten hinweisen und agieren entsprechend. **[wenn zutreffend]**

Schwere der Auswirkung	Maximal			
Eintrittswahrscheinlichkeit	Schulleitung	Sysadmin	Nutzer	Externe
	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar	Eingeschränkt
Risikofaktor	3	3	3	8

9.2.2.3 Risiko Vertraulichkeit

Bedeutung	Wurde Anmeldung an das System mit einem zweiten Faktor (Mehr-Faktor-Anmeldung) für Mitarbeiter implementiert? Wurde die Sichere Links- und Anhänge Technologie implementiert?			
Microsoft 365	Für sämtliche Mitarbeiter-Konten ist Multi-Faktor Authentifizierung **[bitte ergänzen&anpassen]** aktiviert. Es erhalten maximal 2 Mitarbeiter der Schule, 1 Mitarbeiter des Schulträgers und die Fa. **[bitte ergänzen&anpassen],** die von der Schule per Auftragsverarbeitung beauftragt wurde, administrative Rechte.			
Schwere der Auswirkung	Signifikant			
Eintrittswahrscheinlichkeit	Schulleitung	Sysadmin	Nutzer	Externe
	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar	Eingeschränkt
Risikofaktor	3	3	3	6

9.2.2.4 Risiko Transparenz

Bedeutung	Ist sichergestellt, dass die IT Plattform nicht zur Überwachung missbraucht werden kann?			
Microsoft 365	Die Schulleitung hat eine Dienstvereinbarung mit dem Personalrat geschlossen (Muster siehe Muster-Dienstvereinbarung-Schule.pdf (cotec.de)) **[bitte ggf. anpassen]**			
Schwere der Auswirkung	Vernachlässigbar			
Eintrittswahrscheinlichkeit	Schulleitung	Sysadmin	Nutzer	Externe
	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar	Eingeschränkt
Risikofaktor	1	1	1	2

9.2.2.5 Risiko Nichtverkettbarkeit

Bedeutung	Sind Drittanbieter-Apps in Microsoft Teams für weitere Analysen oder weiterer Bearbeitung von Daten deaktiviert?			
Microsoft 365	Diese werden an unserer Schule nicht genutzt und nicht aktiviert.			
Schwere der Auswirkung	Signifikant			
Eintrittswahrscheinlichkeit	Schulleitung	Sysadmin	Nutzer	Externe
	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar
Risikofaktor	3	3	3	3

9.2.2.6 Risiko Intervenierbarkeit

Bedeutung	Sind allen Schülern und Mitarbeitern Ansprechpartner bekannt, die Anmeldedaten ändern können? Wurden Schüler und Mitarbeiter über die Sichtbarkeit von selbst hinterlegten Profildaten informiert?
Microsoft 365	Alle Lehrer können Anmeldedaten von Schülern anpassen und es wurden alle darüber informiert, dass selbst hinterlegte Fotos oder

	Telefonnummern von allen anderen Kontoinhabern gelesen werden können. **[bitte ggf. anpassen]**			
Schwere der Auswirkung	Signifikant			
Eintrittswahrscheinlichkeit	Schulleitung	Sysadmin	Nutzer	Externe
	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar	Eingeschränkt
Risikofaktor	3	3	3	6

9.2.2.6 Risiko Datenminimierung

Bedeutung	Ist gesichert, dass die Konten der Schüler und Mitarbeiter, die die Schule dauerhaft verlassen, nach angemessener Zeit gelöscht werden? Ist sichergestellt, dass Besprechungs-Chats in Teams nach angemessener Zeit gelöscht werden? Ist sichergestellt, dass nur berechtigte Benutzer Zugriff auf Log-Dateien und Berichte haben?			
Microsoft 365	**[Ggf. anpassen]** Schülerkonten: 30 Tage nach dauerhaften Verlassen der Schule, Lehrerkonten: 3 Monate nach Dienstbeendigung. Auf Log-Daten haben ausschließlich definierte Administratoren Zugriff. Jeder Inhaber einer administrativen Rolle oder Funktion in Office 365 wird zur Wahrung der Vertraulichkeit und des Datenschutzes geschult und schriftlich verpflichtet. Sämtliche Auswertungen, die nicht der Systemsicherheit oder Fehlersuche und - behebung dienen (statistische Auswertungen) belassen die standardmäßige Pseudonymisierung. Die Funktion „Microsoft Graph Data Connect“ zum Export von Log-Daten wird nicht verwendet.			
Schwere der Auswirkung	Signifikant			
Eintrittswahrscheinlichkeit	Schulleitung	Sysadmin	Nutzer	Externe
	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar	Signifikant
Risikofaktor	3	3	3	9

Zusätzlich zu den angeführten Risiken sind noch folgende weitere Risiken für die Schule relevant:

[Bitte diese Aspekte ggf. anpassen]

Risiko	**Abhilfemaßnahmen**	**Eintritts-wahrscheinlichkeit**
Teams Besprechungen	Standardmäßig haben alle Teilnehmer an einer Teams-Besprechung gleiche Rechte, was nicht schulkonform ist. Unsere Schule nutzt daher die in Teams vorgesehenen Teams-Richtlinien für Schüler. Diese räumen Lehrern mehr Rechte ein und garantieren, dass Lehrer die Kontrolle vollends behalten.	Vernachlässigbar
Teams Externer Zugriff	Der externe Zugriff erlaubt es Schülern und Lehrern, mit anderen Schulen und Organisationen, die Teams einsetzen, zu kommunizieren. Da diese Kommunikation von externen initiiert werden kann, stellt dies ein Sicherheitsrisiko dar. Aus dem Grund ist standardmäßig der externe Zugriff nur für bestimmte Domänen freigeschaltet, die die Systemadministratoren überwachen.	Vernachlässigbar
Teams Gast-Zugriff	Der Gastzugriff ermöglicht Externen mit privaten E-Mailadressen, an Teams-Besprechungen teilzunehmen, zu	Vernachlässigbar

	denen sie explizit mit Ihrer E-Mailadresse eingeladen werden. Diese Möglichkeit ist auf Lehrer beschränkt, Schüler können keine Gäste einladen.	
Teams anonymer Zugriff	Standardmäßig können anonyme Teilnehmer über einen Link an einer Teams-Besprechung oder einem Teams-Webinar teilnehmen. Diese Möglichkeit ist standardmäßig deaktiviert, wird aber für digitale Elternabende oder Informationsveranstaltungen der Schule zeitlich begrenzt aktiviert. Ein Datenaustausch ist dabei ausgeschlossen.	Vernachlässigbar
Video-Aufzeichnung und Transkription	Videoaufzeichnungen und Transkription sind ausgeschaltet, da sie in der Schule nicht benötigt werden	Vernachlässigbar
Externe und interne Datei-Freigaben	Anonyme Freigaben an Externe sind ausgeschaltet. Nur Lehrer können Daten an externe Nutzer freigeben. Um falsche Freigaben zu verhindern, werden alle Mitarbeiter für die korrekte Konfiguration von Freigaben geschult.	Vernachlässigbar

10. Notwendigkeit der Konsultation nach Art. 36 DSGVO

Durch die identifizierten und anzuwendenden Maßnahmen werden die bei jeglicher Art von Verarbeitung personenbezogener Daten bestehenden Risiken für die Rechte und Grundfreiheiten der betroffenen Personen weitestgehend minimiert.

Durch den Einsatz von Microsoft Teams entsteht kein hohes Risiko für die Rechte und Freiheiten der Mitarbeiter, weder in Teilbereichen noch in der Gesamtheit.

Eine Notwendigkeit zur Konsultation der Aufsichtsbehörde nach Art. 36 Datenschutz-Grundverordnung besteht daher nicht.

11. Fazit

Im Rahmen der Datenschutz-Folgeabschätzung wurde ein Paket an Maßnahmen definiert, die das Risiko für die Rechte und Grundfreiheiten der Betroffenen bei der Verarbeitung personenbezogener Daten zur Verbesserung der Kommunikation und Zusammenarbeit innerhalb der Schule weitgehend reduzieren.

Bei konsequenter Umsetzung der definierten technischen und organisatorischen Maßnahmen werden die zwangsläufig bei der Verarbeitung personenbezogener Daten entstehenden Risiken für die Rechte und Freiheiten der Betroffenen auf ein tragbares Maß reduziert.

Dem Einsatz von Microsoft 365 mit den Diensten Teams , Sharepoint und Exchange Online zur Verbesserung der Kommunikation und Zusammenarbeit in der Schule steht aus Sicht des Datenschutzes nichts entgegen.

Die Einhaltung der getroffenen Maßnahmen und deren Wirksamkeit müssen jedoch regelmäßig und systematisch überprüft, und sich aus der Überprüfung eventuell ergebende Verbesserungen in den Produktionsbetrieb integriert werden.