

Anhang A: Genutzte Microsoft 365-Dienste

Dienstübergreifende Angaben für Löschfristen: Metadaten (Log-Dateien) werden automatisch nach 90 Tagen durch Microsoft gelöscht.

Bezeichnung: Azure Active Directory, Azure Information Protection, Mehrfaktoranmeldung

Funktion	Das Azure Active Directory (AAD) ist der zentrale Verzeichnisdienst für alle Microsoft 365 Anwendungen. Es dient in erster Linie zur Authentifizierung der Benutzer und der Registrierung von Geräten, um Single-Sign-On zu ermöglichen.
Verarbeitete Daten	Pseudonymisierter Name, Pseudonymisierter Vorname, Kürzel (LehrerInnen), Email-Adresse, Tag des Geburtstages bei SchülerInnen, Metadaten zu Anmeldungen und sicherheitsrelevanten Vorgängen (An-Abmeldungen, Rechteänderungen, etc.)
Löschfristen	Benutzerkonten werden beim Ausscheiden eines Beschäftigten deaktiviert und nach 90 Tagen gelöscht.
Überwachungsprotokolle, Anmeldeberichte, Sicherheitsberichte	Dienen der Systemintegrität und Betriebssicherheit, werden nach 90 Tagen gelöscht, Zugriff nur Administratoren
Azure Information Protection	Ermöglicht für AAD-Gruppen eine zertifikatsbasierte Verschlüsselung von Dateien auf allen Endgeräten. Die Dateien können danach nur von Mitgliedern der Gruppe mit den eingestellten Rechten (Lesen oder/und Schreiben) geöffnet werden.
Mehrfaktoranmeldung	Nach Aktivierung erfordert die Anmeldung an Microsoft 365 Dienste in gewissen zeitlichen Abständen die Angabe eines zweiten Faktors wie eine private E-Mailadresse, Telefonnummer, Beantwortung von Fragen oder die Microsoft Authenticator App.

Bezeichnung: Exchange Online und ATP

Funktion	Exchange Online ist eine Groupware- und E-Mail-Transport-Server-Software. Sie dient der zentralen Ablage und Verwaltung von dienstlichen E-Mails, Terminen, Kontakten, Aufgaben und weiteren Elementen für mehrere Benutzer und ermöglicht so die Zusammenarbeit in einer Arbeitsgruppe oder in der gesamten Organisation.
Verarbeitete Daten	Pseudonymisierter Name, Pseudonymisierter Vorname, Kürzel (LehrerInnen), Tag des Geburtstages (SchülerInnen), Email-Adresse, Inhaltsdaten von Email, Kalender und Kontakten, Metadaten zur Kommunikation und Produktnutzung

Löschfristen	Inhaltsdaten werden 90 Tage nach Ausscheiden eines Beschäftigten gelöscht.
Transportregeln	Dienen der Verhinderung von Weiterleitungen an private Konten und werden von den Administratoren erstellt
Postfachüberwachung	Es wird protokolliert, wenn ein Benutzer, bei dem es sich nicht um den Besitzer des Postfachs handelt, auf das Postfach zugreift, zwecks Sicherstellen der Systemintegrität und Vertraulichkeit, Zugriff nur Administratoren
Advanced Threat Protection (ATP)	Es wird jeder Link in E-Mails und Onedrive Dokumenten so umgeschrieben, dass er zum Zeitpunkt des Klicks noch einmal überprüft wird. Zusätzlich wird jeder Anhang in einem virtuellen Container nach aktiven Elementen, die Daten verändern würden, untersucht. Solche Anhänge werden gelöscht.
InPlace Hold, Verhindern von Datenverlust,	Diese Funktionen werden derzeit nicht genutzt
Aufbewahrungsrichtlinien und Journal	Diese Funktionen werden derzeit nicht genutzt

Bezeichnung: Security & Compliance

Funktion:	Microsoft 365 enthält eine Vielzahl von Funktionen, die dabei unterstützen sollen, die Systemsicherheit sowie die Compliance der Organisation sicherstellen zu können.
Verarbeitete Daten:	Pseudonymisierter Name, Pseudonymisierter Vorname, Kürzel (LehrerInnen), Tag des Geburtstages (SchülerInnen), Email-Adresse, Weitere Profileigenschaften eines Benutzers, Metadaten zur Kommunikation und Produktnutzung
Berichte	Zwecks Sicherstellen der Systemintegrität und Vertraulichkeit, Zugriff nur Administratoren
PowerBI, Bezeichnungen, Bezeichnungsrichtlinien, Verhindern von Datenverlust (DLP) Data Governance, Aufsicht und Inhaltssuche	Diese Funktionen werden derzeit nicht genutzt

Bezeichnung: SharePoint Online, OneDrive, Delve

Funktion	SharePoint Online wird indirekt durch Teams oder Microsoft 365 Gruppen oder OneDrive genutzt für die Verwaltung der Zugriffsrechte, von Kalendern und Dokumentenbibliotheken
Verarbeitete Daten	Pseudonymisierter Name, Pseudonymisierter Vorname, Email-Adresse, Kürzel (LehrerInnen), Tag des Geburtsdatums (SchülerInnen), weitere Profileigenschaften eines Benutzers, Inhaltsdaten von Dokumenten und Listen, Metadaten zur Verwendung und Produktnutzung
Löschfristen	In den Papierkorb verschobene Dokumente werden automatisch nach 30 Tagen gelöscht.

Benutzerprofile	enthalten Name, Vorname, Email-Adresse und ermöglichen Kommunikation und Zusammenarbeit. Jeder Beschäftigte kann freiwillig weitere Informationen hinzufügen und löschen. Es wird darauf verwiesen, dies nicht auszufüllen.
OneDrive for Business	Dient der Ablage persönlicher Dokumente, die jeder selbst lesen, schreiben und löschen kann. Fälschlich gelöschte Dateien können über einen Zeitraum von maximal 4 Wochen selbst wieder hergestellt werden. Einzelne Dateien oder Ordner können anderen Benutzern zum Lesen oder zum Lesen und Schreiben freigegeben werden.
Delve	Dient dem leichteren Auffinden relevanter Dokumente und Informationen und zeigt zuletzt benutzte Daten an. Die Anzeige umfasst sowohl eigene Daten als auch durch andere Personen freigegebene Daten. Bei Bedenken bzgl. unbeabsichtigter Freigaben kann Delve von den Administratoren global ausgeschaltet werden.

Bezeichnung: Teams

Funktion	Microsoft Teams ist einerseits eine Whatsapp-ähnliche Chatumgebung mit der Möglichkeit, private 1-zu-1 Chats zu führen und Dokumente und Daten einer Gruppe von Personen zur Verfügung zu stellen. Darüber hinaus ist es durch Einbindung der Klassennotizbücher eine auf OneNote und Formularen basierende Lernplattform mit dem das Lehrer/Schüler-Verhältnis angepassten Zugriffsrechten, Aufgabenzuteilung und Aufgabenbewertung.
Verarbeitete Daten	Pseudonymisierter Name, Pseudonymisierter Vorname, Tag des Geburtsdatums (SchülerInnen), Kürzel (LehrerInnen), Email-Adresse, Weitere Profileigenschaften eines Benutzers, Präsenzinformationen, Metadaten zur Kommunikation und Produktnutzung, Inhalte der Klassennotizbücher, bei Verwendung: Bild und Ton der Webcam.
Löschfristen	Teams mit Klassennotizbüchern der Lehrer und Schüler, die die Klasse/Schule verlassen haben, werden zum Schuljahresende inklusive aller gespeicherten Daten gelöscht.
Richtlinien	Teams inkludiert eine Übersetzungsfunktion, die derzeit noch auf US-Servern ausgeführt wird und daher standardmäßig gesperrt ist.
Konnektoren und Apps	Diese Funktionen werden derzeit nicht genutzt

Bezeichnung: Intune für Bildung

Funktion	Intune ermöglicht mittels des Azure Active Directory die Verwaltung von Geräten, inklusive der Installation von Applikationen, Updates und Richtlinien für Windows 10, Mac OS, iOS und Android.
----------	---

Verarbeitete Daten	Benutzerprofile inklusive zwischengespeicherter One-Drive Dateien, Namen der Rechner, benutzerbezogene Rechtezuweisung für die Nutzung von Geräteeigenschaften und -einstellungen
Löschfristen	Bedarfsabhängig werden Benutzerprofile automatisch gelöscht, da alle Daten in OneDrive gesichert sind. Administratoren können Geräte im Problemfall auf den Auslieferungszustand zurücksetzen.