Datenschutzbezogene Erwägungen
zum Einsatz von Microsoft 365 Education in Schulen

@FJLS.cloud

Datenschutzbezogene "Risiken“ beim Einsatz von MS365 in Schulen

1. Struktur- und funktionsbedingter Datenaustausch zwischen verschiedenen Programmteilen innerhalb des Systems
2. Sammlung funktionsbezogener und persönlicher Daten
3. Anonymisierte Speicherung von Metadaten zur Auswertung der Nutzung des Produktes in den USA
4. Auf Anweisung von Sicherheitsbehörden und nach gerichtlicher Prüfung in Einzelfällen Datentransfer persönlicher Daten in die USA (Zahlen!)
5. Einseitige Veränderung oder Aktualisierung der Nutzungsbedingungen, Vereinbarungen

Aktiver Datenschutz für den schulischen Einsatz von MS365

A	Technische Schutzmaßnahmen

1. Jede Nachricht, alle Anhänge und alle Links werden automatisch auf Schadsoftware geprüft
2. Login mit moderner Authentifizierung (z.B.: Zwei-Faktor möglich)
3. Geoblocking möglich
4. Starke Verschlüsselung von Dateien durch funktional und namentlich frei definierbare Richtlinien (Vertraulichkeitsbezeichner) möglich
5. Richtlinien zur automatischen Löschung bestimmter Daten nach festgelegten Zeitplänen (DSGVO)
6. Kontinuierliche Aktualisierung aller Systembestandteile dabei optimale Anpassung an Windows-Betriebssysteme
7. Verhinderung von Datenverlust, automatische Datensicherung und Bereinigung (Backup)
8. Echter Datenschutz durch automatische Durchführung o.g. datenschutzbezogener Maßnahmen
9. Ausfallschutz durch verteilte Rechenzentren
10. Ausgezeichnete Unterstützung durch den Hersteller

B	Organisatorische Schutzmaßnahmen

1. Jeder Benutzer im System und allen Programmen ist bei entsprechender Nutzung sicher authentifiziert und erkennbar
2. Nachrichtensystem in Teilen oder gänzlich leicht abschirmbar nach außen (z.B. effektive Verhinderung, dass an einzelne Schülerinnen und Schüler, Klassen oder ganze Kollegien Nachrichten von außerhalb der Schule geschickt werden)
3. Administratorrollen ermöglichen Unterstützung der Schülerinnen und Schüler durch technisch-pädagogisches Personal, z.B.: Analyse von Verbindungsproblemen, technischen Problemen beim Einloggen oder der Verwendung von Programmen, vergessenen Passwörtern (organisatorisch-pädagogischer Schutz)
4. Vom System gesammelte Daten können pädagogisch genutzt werden (Lernzeiten, Ordnungsmaßnahmen bei Fehlverhalten)

C	Rechtliche Schutzmaßnahmen

1. Automatische Funktion zur Bereitstellung aller gespeicherten persönlichen Daten im Auskunftsfall nach DSGVO
2. Umfangreiche Unterstützung des Herstellers durch Vorschläge für besseren Datenschutz und Konformität gegenüber bestehenden rechtlichen Richtlinien
3. Regelmäßige Anpassung an aktuelle rechtliche Standards (vgl. Risiko Nr. 5)

Konkrete an der FJLS bereits eingeführte technisch-organisatorische Schutzmaßnahmen

Stand 06.2021

1. Verwendung sicherer Passwörter aus einer Datenbank (Active Directory) für alle schulischen Softwareangebote (Moodle, MS 365 Education, Statista.de, Geogebra) Ausgenommen ist das Hessischen Schulportal (Peadnet und PaedOrg, dort wird die Datenbank eigenständig gepflegt)
2. Passwortrücksetzung nur durch Administration / Lehrkräfte durchführbar
3. Globale Administratorenpasswörter mit Zwei-Faktor-Authentifizierung gesichert
4. Rollenbezogene Administrationsrechte, keine Administratorenrollen für Lehrkräfte
5. Lehrkräfte haben nur Zugriff auf die Daten von den Schülerinnen und Schülern, die sie auch unterrichten und auch nur in den Bereichen, die nachvollziehbar für den Unterricht verwendet werden
6. Kein Zugang zu privaten Datenbereichen der *Nutzerinnen und Nutzer* außer durch globale Administratoren und auch dann nur nach Information der Nutzerinnen und Nutzer (Passwortrücksetzung)
7. Kein Zugriff der Administratoren auf Passwörter der Nutzerinnen und Nutzer
8. Keine strukturelle Speicherung personenbezogener Daten außer Name, Vorname, Jahrgangsstufe, Schulform, belegte Kurse
9. Keine Speicherung privater E-Mailadressen zur Passwortrücksetzung
10. Keine Verbindung von privaten und schulischen Daten (z.B. durch Speicherung von Geburtsdaten, privater E-Mailadressen, postalischer Adressen oder Telefonnummern)
11. Richtlinie zur Datenaufbewahrung: nach Löschung des Accounts werden nach 30 Tagen sämtliche Daten und Dateien, nach 180 Tagen sämtliche Metadaten gelöscht;
12. GeoLock – Einloggen der *Nutzerinnen und Nutzer* mit IP-Adressen aus anderen Staaten als Deutschland ist nicht möglich
13. Speicherungsoption auf europäischen Servern gewählt – im Moment Frankfurt und Amsterdam
14. Automatische Spam- und Virenfilter für sämtliche E-Mails und Dateien vor Speicherung bzw. Übertragung
15. Automatische Versionierung mit Datensicherung für Dokumente im Cloud Speicher
16. Anwendungen deren Daten nicht in Europa liegen, sind für die Benutzung gesperrt (Lizenz zur Nutzung deaktiviert)
17. Anwendungen zur Bildung sozialer Netzwerke außer Teams (z.B. Yammer, LinkedIn-Verbindung) sind deaktiviert
18. Möglichkeit zur Aufzeichnung von Audio- oder Videokonferenzen innerhalb des Systems ist deaktiviert.
19. Störungen von Unterrichtsveranstaltung durch Dritte durch die Weitergabe von Besprechungslinks ist nicht möglich (Zulassung durch Lehrkräfte nötig)
20. Zugang zu Anwendungen, die aufgezeichnete Besprechungen verwalten oder zur Verfügung stellen (Stream), ist deaktiviert
21. Aufzeichnung von Daten Nutzungsanalyse ist per Lizenzentzug administrativ verboten (Education Analytics, Insight)
22. Basisverschlüsselung für ruhende Daten und Transportverschlüsselung durch den Hersteller aktiviert
23. Zusätzliche Verschlüsselung:
    Niederschwellige Verschlüsselungsbezeicher: Datenzugriff mit Verschlüsselung (E-Mail und Dokumente) kann mit zwei Mausklicks auf Personenkreise (SuS, Lehrkräfte, Schulleitung) festgelegt werden. -
    Komplexe zusätzliche Verschlüsselung: Dokumente können durch *Nutzerinnen und Nutzer* mit eigenem Passwort verschlüsselt werden, sodass sowohl Administratoren als auch Microsoft keinen Zugriff nehmen können – Vorsicht: wenn der Schlüssel verloren geht, sind Daten unwiederbringlich verloren und können auch durch Administrationseingriff nicht wiederhergestellt werden.
24. Zwei-Administratorenregelung für Audits vorgesehen
25. Vorbereitung für datenabhängige Rechtsanforderungen nach DSGVO: Möglichkeit für Nutzerinnen und Nutzer einen Auszug der gespeicherten Daten zu erhalten

In Arbeit: Aufbewahrungsbezeichner implementieren, durch die Löschfristen für Dateien und E-Mails vorgegeben oder durch den Nutzer bestimmt werden könne