

Microsoft Office 365 für Bildungseinrichtungen

Datenschutz und Sicherheit

DrVis Software GmbH

www.drvis.de

Microsoft Silver Cloud Partner

Direkter Microsoft Cloud Solution Provider

Mitglied der infoWAN Gruppe

Prof. Dr. Peter Vogl

peter.vogl@drvis.de, Tel: 089 307 48480

Geschäftsführer

MCP, MCIP, MCSE, MCSA Messaging und Office 365

LS Theor. Physik an TUM, em. 2014

Was bietet Office 365? – ein erster Blick

Microsoft 365 Apps: Aktuelles Office Paket für Windows, Mac, iOS, Android, 10 Installationen inklusive

OneDrive for Business: 1 TB Datenspeicher, Synchronisation mit lokalem Gerät, für alle Plattformen

Exchange Online: 50 GB Postfach + Funktionspostfächer + geteilte Kalender + Archiv

Office 365 Gruppen : Konversation+Dokumentenaustausch+Verteiler

Sharepoint Online: Datenbibliotheken mit Versionierung, Kalender, Wikis, Diskussionsforen

Forms: einfache Erstellung und Auswertung von Quizzes, Freitextumfragen, Tests

Sway: Word-ähnliche Erstellung von Dokumenten mit Bildern, Links, Videos mit automatisierter Layout-Erstellung für Handy, Tablet, PC, Mac

Delve: Übersichtliche Darstellung der persönlich aktuellen Projekte und aller Kollaborationen

Zentrale Plattform für Zusammenarbeit: Microsoft Teams

- ❖ Kommunikations- und Lernplattform mit Chat, Daten, Kalender, Audio/Video-Besprechungen, OneNote Klassennotizbücher mit Aufgabenverteilung und –bewertung
- ❖ Fasst Exchange, Sharepoint, und alle anderen Dienste zu einer einheitlichen Benutzeroberfläche zusammen. Es erfordert eine Exchange + Sharepoint Lizenz.

Was bietet Office 365? – ein erster Blick

Insgesamt ca. 200 Dienste und zusätzlich ca. 1500 Dienste in Azure

- Alle Komponenten können individuell und einzeln lizenziert (= ein/ausgeschaltet) werden
- Mit Ausnahme von Microsoft 365 Apps sind alle Dienste für Schulen kostenlos

❖ Schutz gegen Phishing, Ransomware, Trojaner in E-Mail durch erweiterte Schutzfunktionen:

Sichere Links-Technologie: Links in E-Mails und Dokumenten werden umgeschrieben, sodass sie im Zeitpunkt des Klicks nochmal vom Exchange Online Protection Server überprüft werden

Sichere Anhänge-Technologie: Anhänge werden in dynamisch erzeugter virtueller Maschine geöffnet. Wenn der Anhang Daten verändert, wird er gelöscht.

❖ Schutz gegen Identitätsdiebstahl:

Office 365 unterstützt eine komfortable **Multi-Faktor-Authentifizierung** (analog zu M-TAN), sodass ein Diebstahl des Passworts wirkungslos bleibt

❖ Schutz gegen Datendiebstahl:

Office 365 unterstützt die durchgängige Ende-zu-Ende Verschlüsselung von Daten in allen Diensten. Beispielsweise kann eine Worddatei mit einem Klick so verschlüsselt werden, dass sie nur Mitarbeiter der Schule öffnen können. Damit können MA sensitive Daten anlegen, bearbeiten und Kolleginnen oder Kollegen zugänglich machen (**“Azure Information Protection”**).



- ❖ ATP schützt Dateien in Sharepoint, OneDrive, Teams und Forms
- ❖ Anlagen mit aktiven Elementen werden entfernt und gelöscht
- ❖ Links werden umgeschrieben, sodass sie zum Zeitpunkt des Klicks nochmal überprüft werden
- ❖ ATP hängt nicht ab von Virensignaturen

Exchange Admin Center

Dashboard

Empfänger

Berechtigungen

Complianceverwaltung

Organisation

Schutz

Komplexe Bedrohungen

Sichere Anlagen Sichere Links

Verwenden Sie diese Seite, um Ihre Organisation vor bösartigen Inhalten in E-Mail-Anlagen und Dateien in SharePoint, auf OneDrive und in Microsoft Teams zu schützen.

Dateien in SharePoint, auf OneDrive und in Microsoft Teams schützen

Wenn in einer der SharePoint-, OneDrive- oder Microsoft Teams-Bibliotheken eine Datei als bösartig identifiziert wird, hindert ATP Benutzer am Öffnen und Herunterladen der Datei. [Weitere Informationen zu ATP für SharePoint, OneDrive und Microsoft Teams](#)

ATP für SharePoint, OneDrive und Microsoft Teams aktivieren

E-Mail-Anlagen schützen

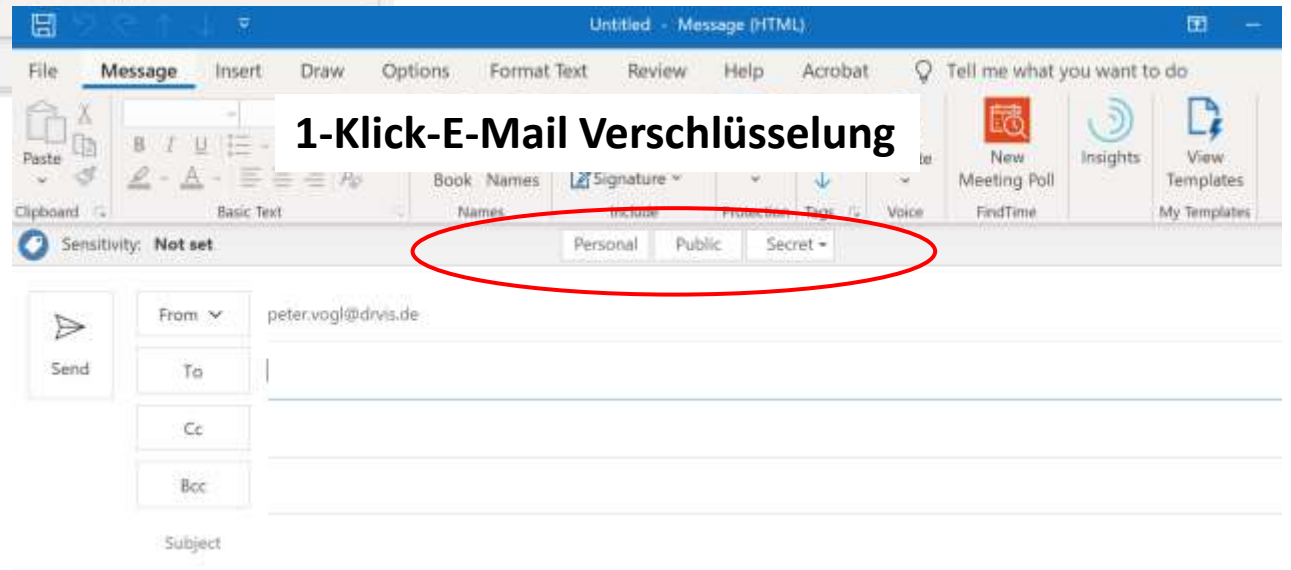
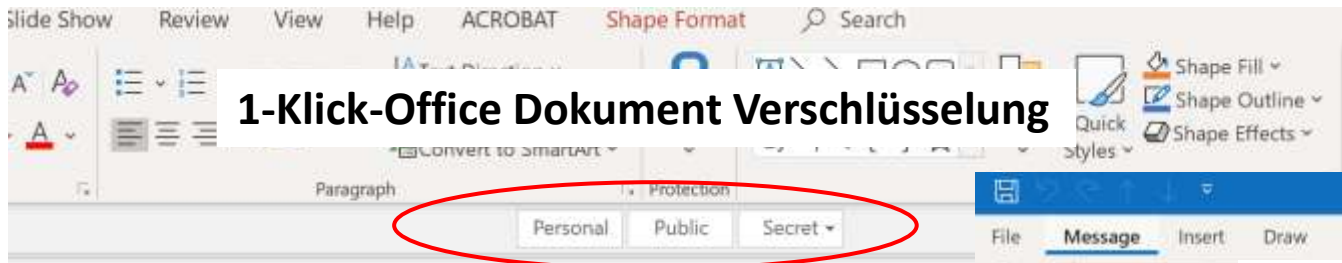
Richten Sie eine ATP-Richtlinie für sichere Anlagen für bestimmte Benutzer oder Gruppen ein, um Personen daran zu hindern, E-Mail-Anlagen zu öffnen oder te die bösartige Inhalte enthalten. [Weitere Informationen zu ATP-sicheren Anlagen für E-Mail](#)

- MFA schützt nicht nur explizite Anmeldung an Office 365, sondern auch verknüpfte Daten und Links
- Sehr komfortabel: bei gleichbleibender Nutzung nur alle 60 Tage 2. Faktor nötig, sofern Gerät im Azure-AD registriert ist (z. B. durch Installation der Microsoft 365 Apps)
- MFA kann individuell oder global eingestellt werden
- Methoden: Festnetztelefon, SMS, Microsoft Authenticator App, Hardwaretoken (FIDO2-Geräte)
- Interne IP-Bereiche können ausgenommen werden („bedingter Zugriff“)



Azure Information Protection (Ende-zu-Ende Verschlüsselung)

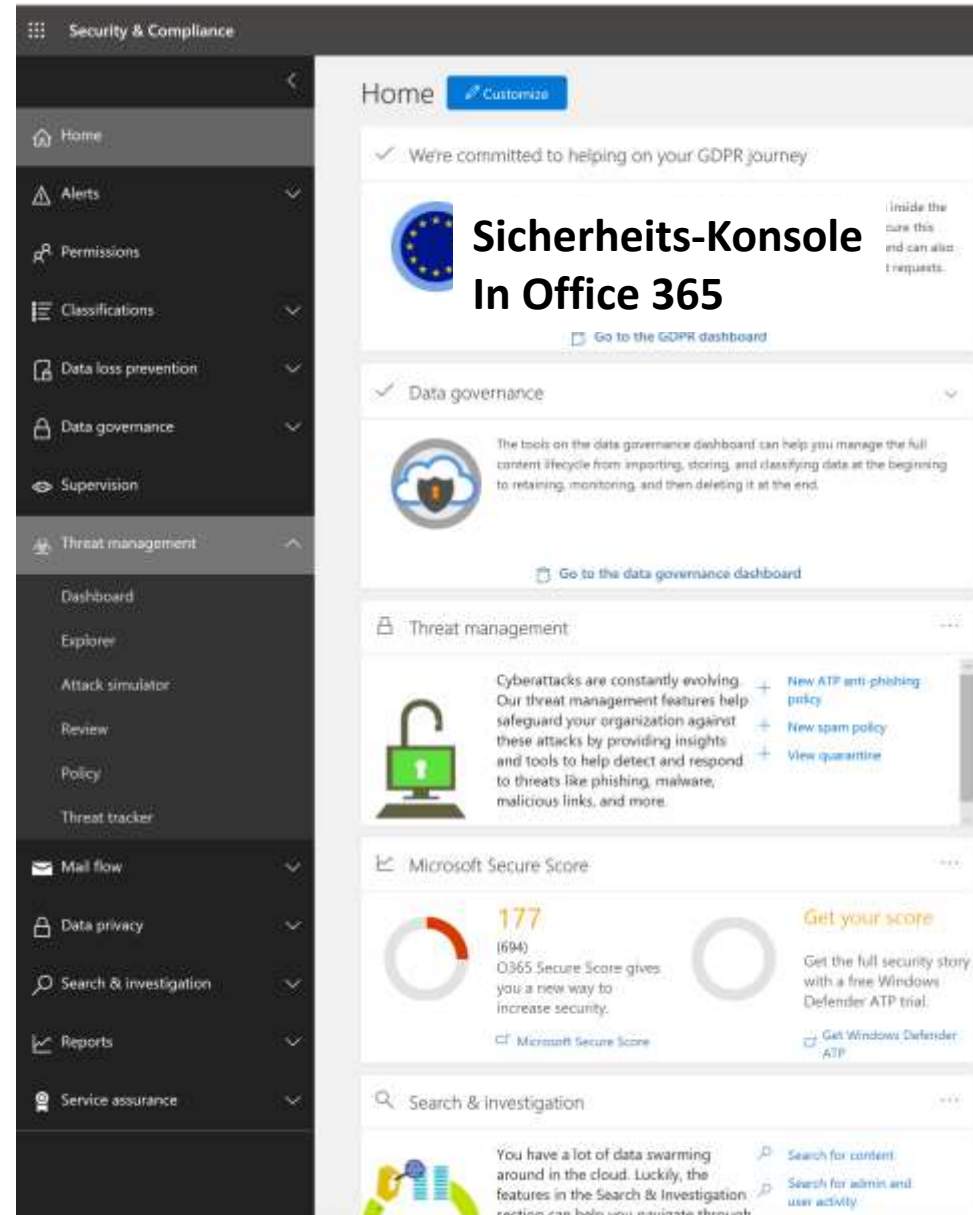
- ❖ Voraussetzung: Gerät muss im Azure AD registriert sein, am einfachsten durch Installation der Microsoft 365 Apps
- ❖ Alle Applikationen können geschützt werden, besonders komfortabel Office Apps:



Administrator kann Richtlinien setzen:

- ❖ Automatische Verschlüsselung für best. Gruppen
- ❖ Zugriffsrechte Lesen/Schreiben/Löschen/...
- ❖ Rechte können zeitlich befristet werden
- ❖ Offline-Zugriff für N Tage möglich

- ❖ Klassifiziert und beschränkt die Ausführung von Applikationen nach Speicherort, Hersteller, Zertifikat: **Cloud App Security**
- ❖ Angriffs-Simulator zur Überprüfung von Schwachstellen im eigenen Netzwerk
- ❖ Schutz gegen Freigabe vertraulicher Daten in E-Mails oder Links
- ❖ Vorschläge zu DSGVO Konformität: z. B. sind Löschregeln hinterlegt? Sind Zugriffsrechte beschränkt? ...
- ❖ Auditing sämtlicher administrativer Tätigkeiten durch speziell eingerichtete Administrator-Konten mit Audit-Rechten



The screenshot displays the Microsoft Security & Compliance Center interface. On the left is a dark navigation pane with options like Home, Alerts, Permissions, Classifications, Data loss prevention, Data governance, Supervision, Threat management, Dashboard, Explorer, Attack simulator, Review, Policy, Threat tracker, Mail flow, Data privacy, Search & investigation, Reports, and Service assurance. The main content area shows a 'Home' dashboard with a 'Customize' button. It features a GDPR journey banner, a 'Sicherheits-Konsole In Office 365' section with a European Union flag icon and a 'Go to the GDPR dashboard' link, a 'Data governance' section with a cloud and shield icon and a 'Go to the data governance dashboard' link, a 'Threat management' section with a padlock icon and links for 'New ATP anti-phishing policy', 'New spam policy', and 'View quarantine', a 'Microsoft Secure Score' section showing a score of 177 (694) and a 'Get your score' link, and a 'Search & investigation' section with a magnifying glass icon and links for 'Search for content' and 'Search for admin and user activity'.

Wo liegt Office 365?

- Mit Nutzung von Office 365 schließen Sie einen AV Vertrag nach DSGVO mit Microsoft Irland : Alle Nutzdaten bleiben vertragsgemäß in der EU (*data at rest*-Klausel) und sind maschinell verschlüsselt
- Alle Daten deutscher Kunden liegen in den neuen Microsoft Rechenzentren Frankfurt und Berlin



Sicherheitsniveau in den EU Rechenzentren von Microsoft

- Frankfurt und Berlin sichern sich gegenseitig ab bzgl. Energie und Datenfluss
- Systeme innerhalb der Rechenzentren sind mehrfach redundant: alle Daten liegen auf virtuellen Servern und jede virtuelle Instanz ist 6-fach gesichert
- Gesamte Datenkommunikation intern und intern-extern erfolgt verschlüsselt
- Die Abwehrsysteme werden 24/7 überprüft und durch eigene Teams („blue“ und „red“) laufend herausgefordert und an neue Bedrohungen angepasst.
- Weltweit höchste Zertifizierung (SAS70, ISO 27001 + 27002 + 27018) für den RZ-Betrieb. Die jährlichen Audit-Protokolle sind am Internet frei zugänglich.
- Der ISO/IEC 27018-Standard wurde von der ISO entwickelt, um in der Cloud gelagerte personenbezogene Daten zu schützen. Microsoft hat als erster führenden Anbieter von Cloud-Diensten diesen Standard global implementiert.
- Garantierte Verfügbarkeit von 99,9%

Was macht Microsoft mit Ihren Daten?

- **Keinerlei inhaltliche Datenanalyse, keinerlei Weitergabe von Kundendaten**
- **Diagnosedaten können Sie mit einer kostenlosen App ([Diagnosedatenanzeiger](#)) aus dem Microsoft Store überprüfen und abschalten**
- **Microsoft erlaubt Kunden clientseitige Verschlüsselung**
- **Daten können mit eigenem Zertifikat in den RZ von Microsoft verschlüsselt abgelegt werden**
- **<http://trustcenter.office365.de> bietet klare Informationen**
 - **wo sich die Daten eines Kunden befinden,**
 - **wer Zugang zu diesen Daten hat,**
 - **wie Microsoft diese Daten schützt,**
 - **welche Zertifizierungen Microsoft erfüllt**
- **AV-Vertrag (Online Services Terms: <https://www.microsoft.com/licensing/product-licensing>)**
 - **Anhang zu den Datenschutzbestimmungen für Onlinedienste: <https://aka.ms/dpa>**
 - **Enthält alle Regelungen zu Art. 28 DSGVO**
 - **Mit EU Datenschutzbehörden bis ins letzte Detail (Jan 2020) abgestimmt**
 - **Enthält die EU-Standardvertragsklauseln**

- ✓ Schutz vor Angriffen auf Applikationen und Plug-Ins
- ✓ Zugriff von Apps nur auf zugelassene Ordner (**Cloud App Security**)
- ✓ Nur explizit zugelassene Applikationen starten (**Cloud App Security**)
- ✓ Schutz des Netzwerks gegen Verbindungen zu fragwürdigen Zieladressen
- ✓ Applikations-Isolation
- ✓ Heuristische Analyse von Inhalten aus fragwürdigen Quellen
- ✓ Windows Defender Antivirus erkennt Schadware nach vielen Kriterien und Verhalten des Geräts mittels Maschinenlernen und Speicheranalyse
- ✓ Edge-Browser:
 - ✓ blockiert Downloads basierend auf Reputationsanalyse und KI
 - ✓ Mit **Windows Defender Application Guard** läuft Edge Browser in eigener virtuellen Maschine ohne Zugriff auf das System
- ✓ OneDrive for Business ermöglicht Versionierung und Rücksetzung aller Daten auf Stand zu früheren Zeitpunkt

Wirksamer Schutz erfordert die laufende Analyse riesiger Datenmengen, um Angriffe frühzeitig erkennen zu können und Gefahren abzuwenden. Dies erfordert große, zentrale Rechenzentren.

Kosten für Energie, Konfiguration, Überwachung, Zertifizierungen:

Microsoft investiert 1 Milliarde Euro pro Monat in den Schutz der gespeicherten Daten.

- Cyberkriminalität erzielte 2018 über 1,5 Billionen Euro Gewinn
- Im Mittel gibt es alle 39 Sekunden einen erfolgreichen Hackerangriff
- Staaten sind beteiligt: über 2 Millionen Menschen arbeiten in der Auslandsspionage, manche Staaten beziehen den Großteil Ihrer Devisen durch Cyberkriminalität
- Schulen und Unis sind ein Brückenkopf zu Firmen und meist schlecht geschützt



Who are us?
We are a professional team. We have programming skills in developing tools. The goal is to provide the highest quality services and make them available.
We also accept the terms of this agreement to develop the services.
And of course we will do our best.

We sell Ransomware
Developed by us. You can use it to ransomware your data and files.

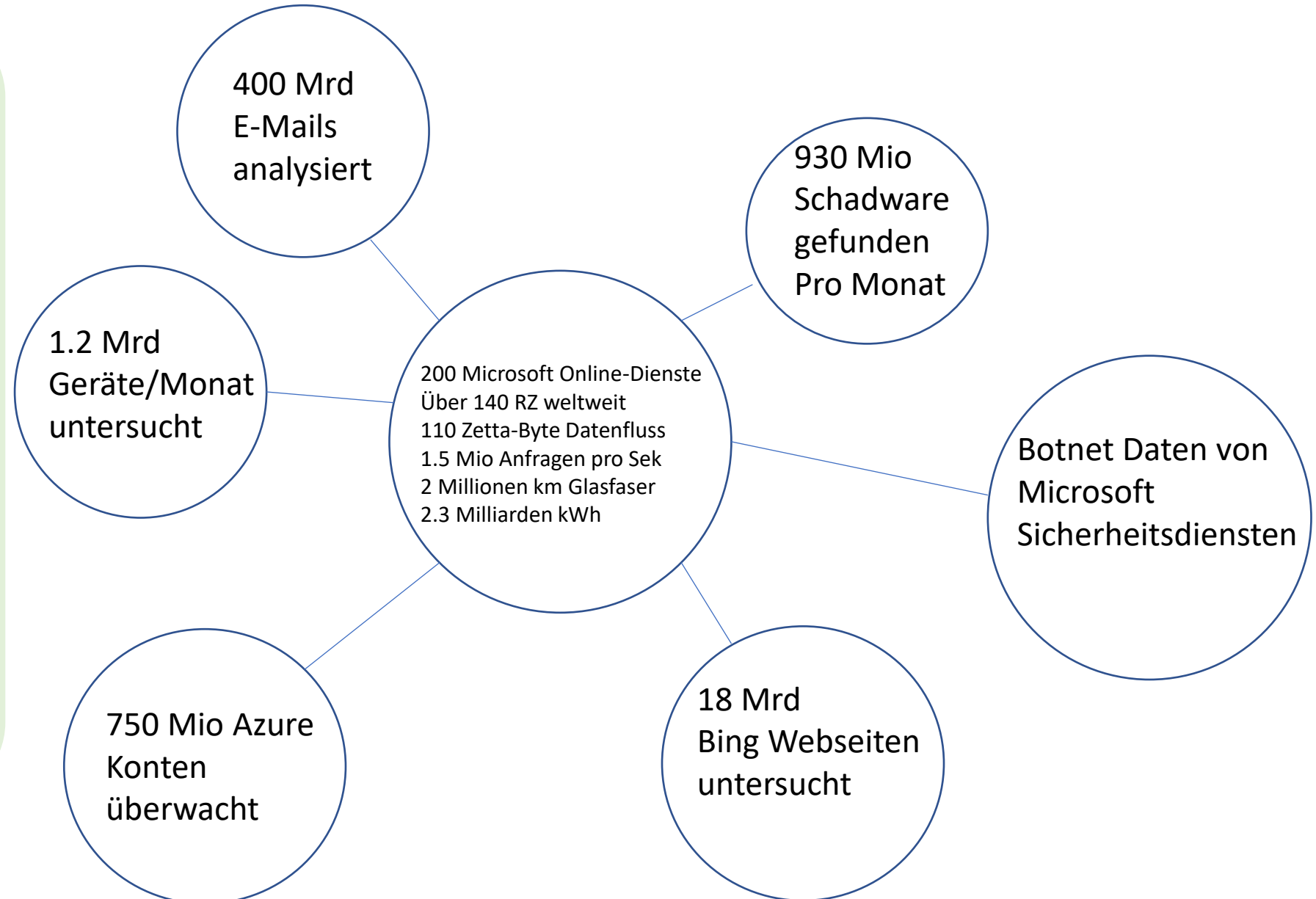
Failure is not an option
We have unlocking solutions!
Do not miss your data.



Sicherheit erfordert gigantischen Aufwand

Wirksamer Schutz erfordert die laufende Analyse riesiger Datenmengen, um Angriffe frühzeitig erkennen zu können und Gefahren abzuwenden. Dies erfordert große, zentrale Rechenzentren.

Kosten für Energie, Konfiguration, Überwachung, Zertifizierungen:
Microsoft investiert 1 Milliarde Euro pro Monat in den Schutz der gespeicherten Daten.



Artikel 1 Gegenstand und Ziele

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

➤ **Datenschutzrechtlich keine Bevorzugung von „Server in Deutschland“**

Sie müssen als Bildungseinrichtung nach Artikel 32 belegbar Auskunft geben können, welche Maßnahmen in technischer und organisatorischer Hinsicht getroffen wurden, um die DSGVO einzuhalten. Eine der wesentlichen Änderungen betrifft die Anforderungen an technische Schutzmaßnahmen. Diese müssen „dem aktuellen Stand der Technik“ entsprechen. Dies bedeutet eine vollkommene Abkehr vom bisherigen Prinzip „my home is my castle“, das in dem 30 Jahre alten BSDG vertreten wurde.

➤ **Trifft für Schul-IT nicht zu.**

Für die Auswahl von IT Dienstleistern („Auftragsverarbeiter“) muss eine Schule nach Art. 28 konkret nachweisen können, dass die Auswahl nach objektiven datenschutzrechtlichen Kriterien erfolgt ist, z. B. durch eine Zertifizierung des Anbieters. Die Microsoft EU Rechenzentren sind nach dem Datenschutz-Standard ISO 27018 zertifiziert.

➤ **Schule sollte zertifizierte Cloudanbieter wählen, z. B. Microsoft Office 365**

Wer darf einer Bildungseinrichtung IT Dienste anbieten, bei denen personenbezogenen Daten verarbeitet werden?

Die DSGVO setzt sich erstmals mit den dramatisch wachsenden Gefahren durch technische Sicherheitslücken auseinander und anerkennt, dass nur sehr große, professionell betriebene und entsprechend ausgestattete Rechenzentren über die Mittel verfügen, den wachsenden Bedrohungen wirksame Schutzmaßnahmen entgegensetzen zu können.

Für die Auswahl von IT Dienstleistern („Auftragsverarbeiter“) gelten in der DSGVO daher wesentlich strengere Maßstäbe:

Artikel 28 (1): „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen („TOM“) so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt ...“. Dies kann durch ... Zertifizierungen und durch die bestätigte Erfüllung der Standarddatenschutzklauseln ... nachgewiesen werden

Welche Zertifizierungen besitzen die Microsoft Rechenzentren?

Internationale Standards	Industrie-Standards	Regionale Standards
Auswahl wichtiger Zertifikate (LINK)		
<ul style="list-style-type: none"> • CSA-STAR Attestation • CSA-STAR Certification • CSA STAR Self-Assessment • DFARS • ISO 20000-1:2011 • ISO 22301 • ISO 27001 • ISO 27017 • ISO 27018 • ISO 9001 • SOC 1, 2 und 3 • WCAG 2.0 • FISMA 	<ul style="list-style-type: none"> • TISAX • BaFin (BAIT) • DPP (UK) • FACT (UK) • FCA (UK) • NEN-7510 (Netherlands) • NHS IG Toolkit (UK) 	<ul style="list-style-type: none"> • BSI C5 (Deutschland) • BIR 2012 (Niederlande) • EN 301 549 (EU) • ENISA IAF (EU) • ENS (Spain) • EU-Standardvertragsklauseln (EU Model Clauses) • EU-US Privacy Shield (EU) • LOPD (Spanien) • PASF (UK) • UK G-Cloud (UK) • IDW PS 951 (Deutschland)* • IT Security Act (Deutschland)* • IT-Grundschutz-Kompendium (Deutschland)*

*) Geplant nach Fertigstellung RZ Frankfurt+Berlin

- Die Bildungseinrichtung (oder der Schulträger) schließt einen Vertrag zur Auftragsverarbeitung mit Microsoft Irland gemäß DSGVO ab, der die EU Standardvertragsklauseln enthält. Die Speicherung der Nutzdaten erfolgt nur innerhalb Deutschlands und die Daten verlassen die EU nicht (= Inhalt der EU Standardvertragsklauseln).
- Microsoft Rechenzentren sind nach strengsten internationalen Standards zertifiziert (= Art 32)
- Alle Nutzdaten sind server- und verbindungsseitig verschlüsselt. Die gespeicherten Daten können zusätzlich Ende-zu-Ende verschlüsselt werden (= Art. 6 (4)e).
- Für die Inhalte ist der Auftraggeber selbst verantwortlich. Wir empfehlen einen Beschluss der Schulkonferenz zur Nutzung von Office 365 und die Anlage eines Verfahrensverzeichnis des Verantwortlichen (Muster auf <https://www.drvis.de/Office365/Basis/5>)
- Damit kann Office 365 datenschutzkonform in der Schule eingesetzt werden.

Ausführliche Diskussion: <https://www.drvis.de/Office365/Basis/4>
(Speicherort, Support-Zugriff, Weitergabe an US-Behörden, Cloud-Act, ...)

Juristische Problematik:

1. Sind verschlüsselte personenbezogene Daten immer noch personenbezogen?
2. Sind anonymisierte Daten wie IP-Adressen grundsätzlich personenbezogen?

Technische Problematik:

- Ohne Telemetriedaten lässt sich ein komplexes Softwareprodukt nicht anbieten und nicht sinnvoll weiterentwickeln
- Es besteht ein Konflikt zwischen praktischer Nutzbarkeit, Transparenz und Technik

Föderalismus Problematik:

- Die 16 Landesdatenschutzbehörden lehnen eine gemeinsame Stellungnahme zu Clouddiensten bisher ab, wird aber angestrebt

- ❖ Microsoft hat sich der DSGVO nicht nur in der EU, sondern weltweit unterworfen, hat anerkannt, dass auch anonymisierte Daten wie IP-Nummern personenbezogen sein können
- ❖ Microsoft publiziert laufend in großem Detail die Telemetriedaten für Office, Windows, Browser am Internet, siehe <https://www.drvis.de/Office365/Basis> und <https://news.microsoft.com/de-de/datenschutz-microsoft/> und ermöglicht deren Abschaltung
- ❖ Microsoft aktualisiert auch laufend die Installationsroutinen, um Transparenz und ausreichend Wahlmöglichkeiten anzubieten.

Beispiel:

- ❖ Nach Einwänden der NL Datenschutzbehörde wegen der Telemetriedaten für Office und Windows hat Microsoft die Möglichkeit geschaffen, diese komplett abzuschalten
- ❖ Die NL Datenschutzbehörde empfiehlt seitdem explizit Office 365 und Windows 10
<https://blogs.microsoft.com/eupolicy/2019/07/02/how-microsoft-works-with-customers-to-keep-their-trust-a-story-from-the-netherlands/>
- ❖ Das LDA Bayern hat bestätigt, dass Windows 10 datenschutzkonform eingesetzt werden kann:
https://www.lda.bayern.de/media/baylda_report_09.pdf (Seite 22)

Diese Prozesse werden allerdings immer laufende Anpassungen und Diskussionen erfordern. Allerdings müssen die Behörden auch bereit sein, Ihre Bedenken konstruktiv Microsoft mitzuteilen.

❖ BayEUG Art. 85 Verarbeitung personenbezogener Daten

(1) Die Schulen dürfen die zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlichen Daten verarbeiten. .. Mit Bezug zu Art. 6 **BayDSG** und **DSGVO**

➤ Rechtmäßigkeit der Verarbeitung folgt aus dem Bildungsauftrag der Schule

❖ Bekanntmachung über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen: <https://www.gesetze-bayern.de/Content/Document/BayVwV270311-16#BayVwV270311-19>

4.3 Datenverarbeitung auf privaten Rechnern der Lehrkräfte

Es ist geeignete Vorsorge zu treffen, dass alle gespeicherten Daten beim Ausfall des Rechners trotzdem jederzeit zur Verfügung stehen.

➤ Das ist nur mit einem automatischen Synchronisationsdienst wie OneDrive möglich

4.4 Auftragsdatenverarbeitung

Die Schule muss den Auftragnehmer sorgfältig auswählen und mit dem Auftragnehmer schriftlich eine Auftragsdatenverarbeitungsvereinbarung abschließen und den Nachweis der Einhaltung der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten Standards zu verlangen – beispielsweise durch Vorlage einer ISO 27001 Zertifizierung

➤ Wird von Office 365 erfüllt

Situation in Bayern: 2 Datenschutzbehörden

Bayerisches Landesamt für Datenschutzaufsicht: <https://www.lida.bayern.de/de/faq.html>

Frage: Wir verwenden einen Cloud-Dienst, um Dateien zu speichern und mit anderen Nutzern zu teilen. Die Datenverarbeitung findet in den USA statt, weil der Dienstleister dort seinen Sitz hat. Ist das zulässig?

Antwort: Ja. Grundsätzlich dürfen Cloud-Dienste verwendet werden. Zu beachten ist, dass mit dem Dienstleister in der Regel ein Vertrag zur Auftragsverarbeitung zu schließen ist. Viele US-amerikanische Dienstleister sind zudem EU-US-Privacy-Shield zertifiziert.

- Empfiehlt professionelle Cloud-Dienste mit angemessenen AV-Vertrag

Bayerischer Landesbeauftragte für den Datenschutz: <https://www.datenschutz-bayern.de/tbs/tb26/k13.html>

Dr. Petry: „Bei mir von Behörden zur Beratung vorgelegten Vertragsbedingungen von Cloud-Anbietern konnte ich feststellen, dass die Anforderungen so nicht erfüllt wurden. Zu anderen Vereinbarungen waren solche Cloud-Anbieter offenbar nicht gewillt.“

- Viele EU Länder und die Schweiz haben eigene Vertrags-Zusätze. Dazu müssten die deutschen DS-Behörden eine gemeinsame Stellungnahme mit Änderungswünschen vorlegen.

Zusammenfassung: Es gibt in Bayern weder Gesetze noch Verordnungen, die Schulen den Einsatz von Office 365 verbieten.

- ❖ Lokale Server in Schulen stellen eine grob fahrlässige Verletzung der DSGVO dar, da sie weder professionell betrieben noch zertifiziert sind.
- ❖ Telemetriedaten benötigt jedes IT-System, Windows, Apple, Google usw. Microsoft dokumentiert dies sehr ausführlich und ermöglicht deren Abschaltung. Dies hat nichts mit Office 365 zu tun.
- ❖ Cloud-Dienste für Privatkunden wie WhatsApp, Facebook, Apple Cloud werden mangels attraktiver Alternativen in vielen Schulen eingesetzt. Dies ist auf Dauer nicht akzeptabel.
- ❖ Die historisch gerätebezogene Zuweisung von Lizenzen, Applikationen und Daten („mein PC“, „unser Server“) ist nicht mehr zeitgemäß und für einen IT-gestützten Unterricht ungeeignet. Der Schüler und Lehrer benötigt die Apps und Daten orts- und geräteunabhängig. Dies erfordert eine professionell betriebene Cloud.
- ❖ Mit Office 365 schließt die Bildungseinrichtung einen Auftragsverarbeitungsvertrag mit MS Irland gemäß DS-GVO, der die EU Standardvertragsklauseln enthält.
- ❖ Speicherung der Nutzdaten erfolgt in Deutschland.
- ❖ Alle Nutzdaten sind server- und verbindungsseitig verschlüsselt und zusätzlich individuell Ende-zu-Ende verschlüsselbar.
- ❖ Für die Inhalte ist der Auftraggeber selbst verantwortlich.