co.Tec
Software. Hardware. Bildung.

Microsoft Office 365

Wichtige Infos zu Datenschutz und Sicherheit

Agenda

Wer ist co.Tec?

co.Tec macht Bildung digital – seit 30 Jahren. Als einer der führenden deutschen Händler von Hard- und Software für den Bildungsbereich stellt das Rosenheimer Unternehmen Lösungen bereit, die das digitale Lehren und Lernen an Schulen fördern. Das hochwertige Produktportfolio umfasst 80 namhafte Marken wie unter anderem Microsoft, HP, Adobe und Acer. Ergänzt wird das Angebot durch diverse Serviceleistungen rund um das Thema Cloud. Als ganzheitlicher Lösungsanbieter für das Thema **#Schultransformation** liefert co.Tec Antworten auf Ihre Fragen rund um die Digitalisierung von Schulen und steht Ihnen mit Rat und Tat zur Seite.

Der **#Digitalpakt** ist für uns mehr als nur Zukunftsmusik. Wir sind der richtige Partner, um die Digitalisierung an deutschen Schulen voranzutreiben. Auch an Ihrer Schule.

#Office 365

Was bietet Office 365?

Was bietet Office 365

Office 365 ProPlus	Aktuelles Office Paket für jede Plattform (“Office 365 ProPlus
OneDrive for Business	1 TB Datenspeicher, Synchronisation mit lokalem Gerät, für alle Plattformen
Office 365 Gruppen	Konversation+Dokumentenaustausch+Verteiler
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
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.

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

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

#Office 365

5 Gründe, warum Office 365 datenschutzkonform ist

1. Höchste Sicherheit nach Stand der Technik

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

- Sichere Links-Technologie: Links in E-Mails und Dokumenten werden umgeschrieben, sodas sie im Zeitpunkt des Klicks nochmal vom Exchange Online Protection Server überprüft werden
- Sichere Anhänge-Technologie: Anhänge werden in dynamisch erzeugter virtuellen Maschine geöffnet. Wenn der Anhang Daten verändert, wird er gelöscht.

Schutz gegen Identitätsdiebstahl:

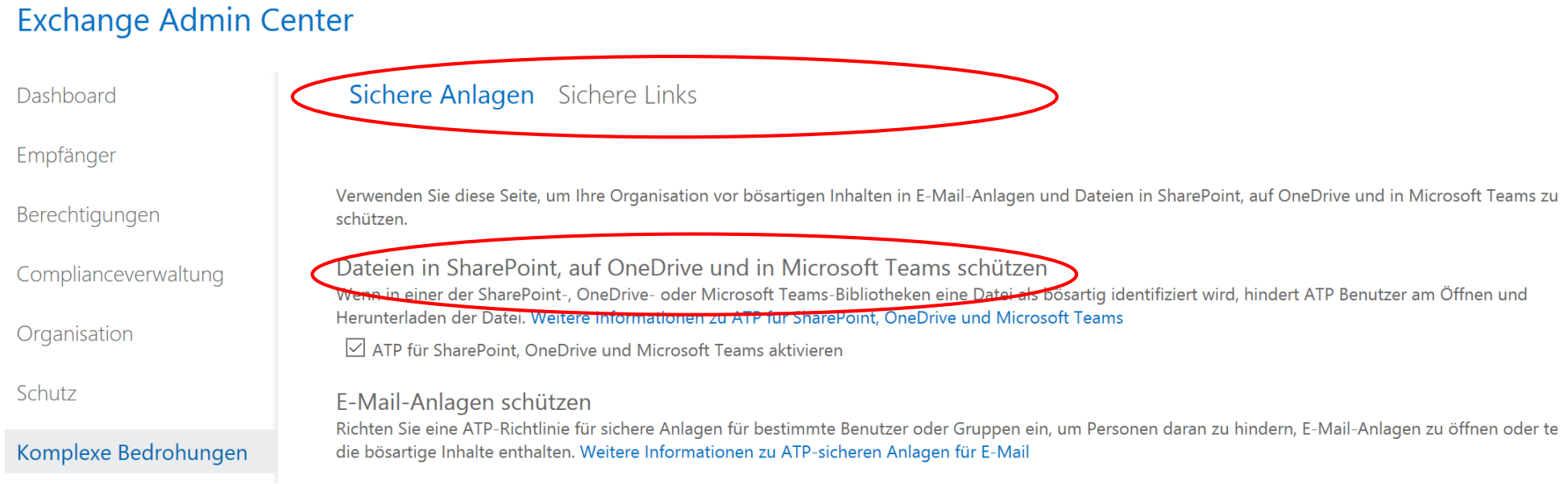
Office 365 unterstützt eine komfortable Multi-Faktor-Authentifizierung (analog zu M-TAN), sodass ein Diebstahl des Passworts wirkungslos bleibt

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”).

2. Advanced Threat Protection („Komplexe Bedrohungen“)

- 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



3. Mehrfaktoranmeldung

- 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 von Office 365 ProPlus)
- MFA kann individuell oder global eingestellt werden
- Methoden: Festnetztelefon, SMS, Microsoft Authenticator App, Hardwaretoken (FIDO2-Geräte)
- Interne IP-Bereiche können ausgenommen werden („bedingter Zugriff“)

Security Key by Yubico

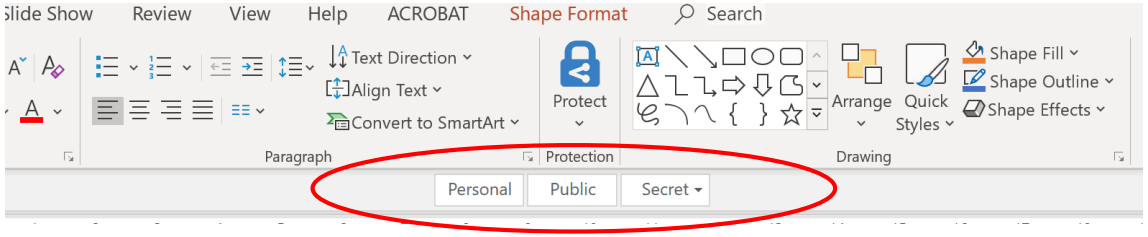
Yubico

4. Azure Information Protection

(Ende-zu-Ende Verschlüsselung)

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

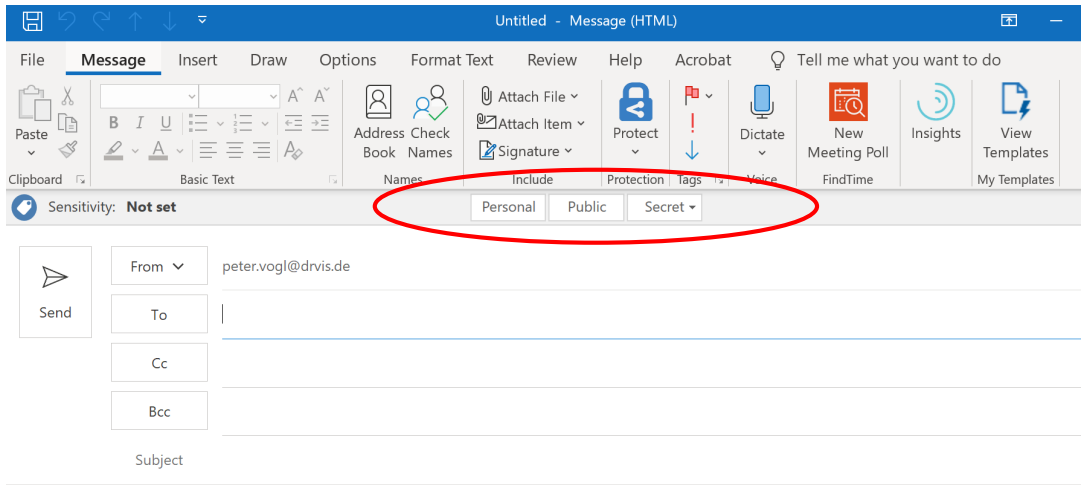
1-Klick-Office Dokument Verschlüsselung



Administrator kann Richtlinien setzen:

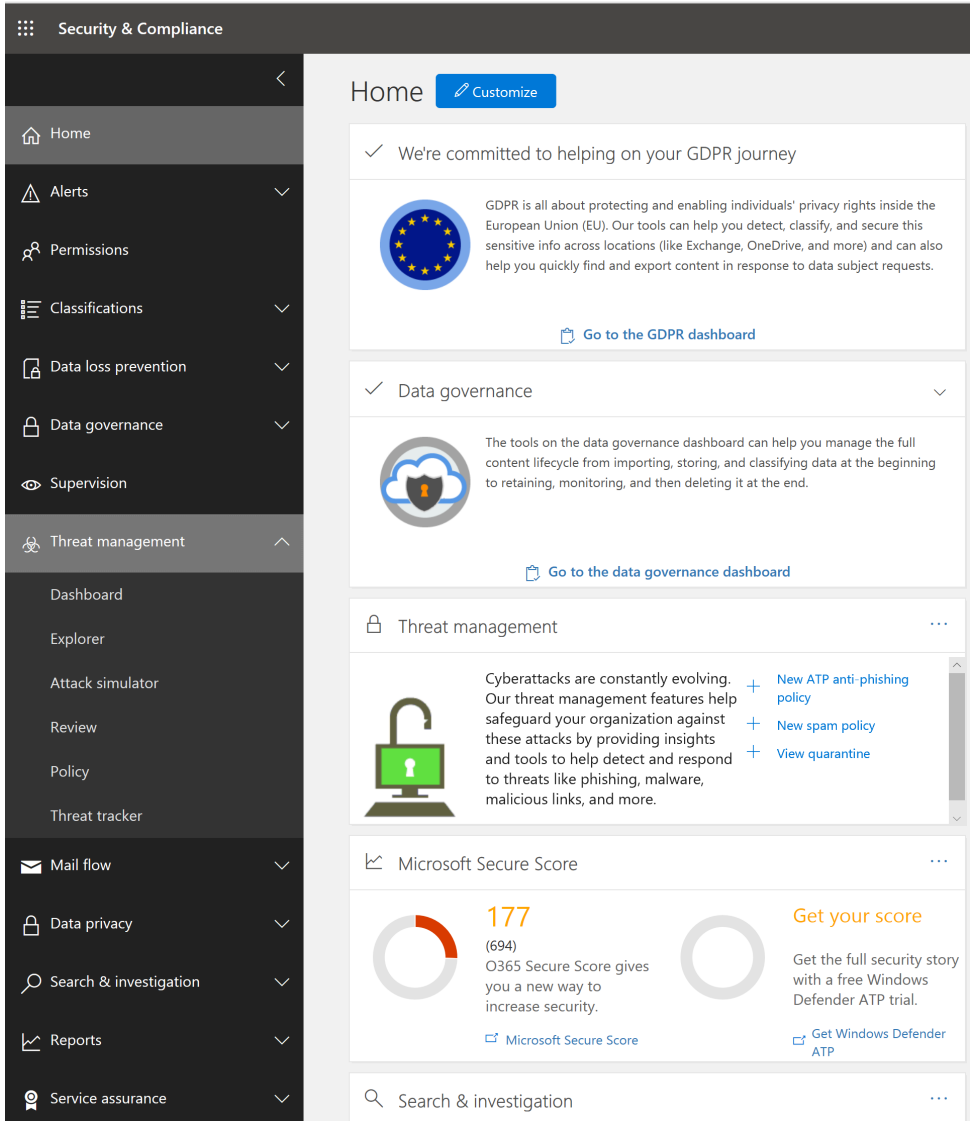
- Automatische Verschlüsselung für best. Gruppen
- Zugriffsrechte Lesen/Schreiben/Löschen/…
- Rechte können zeitlich befristet werden
- Offline-Zugriff für N Tage möglich

1-Klick-E-Mail Verschlüsselung



5. Sicherheits-Konsole in Office 365

- 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



#Office 365

Auftragsdatenverarbeitung (ADV) und Cloud-Vertrag?

Was passiert mit Ihren Daten?

- Keinerlei inhaltliche Datenanalyse, keinerlei Weitergabe von Kundendaten
- Diagnosedaten können Sie mit einer kostenlosen App (Diagnosedatenanzeiger) aus dem Microsoft Store selbst überprüfen
- 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: http://aka.ms/Wkcowi)
  - Enthält alle Regelungen zu Art. 28 DSGVO
  - Enthält die EU-Standardvertragsklauseln

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

Microsoft Rechenzentren in Europa

In Bälde zusätzlich: Berlin und Frankfurt

Welche Zertifizierungen besitzen die Microsoft Rechenzentren?

Internationale Standards	Industrie-Standards	Regionale Standards
Auswahl wichtiger Zertifikate (LINK)		
• 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	• TISAX • BaFin (BAIT) • DPP (UK) • FACT (UK) • FCA (UK) • NEN-7510 (Netherlands) • NHS IG Toolkit (UK)	• 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

Sicherheitsniveau der Microsoft Rechenzentren

- Dublin und Amsterdam (bzw. Berlin und Frankfurt) 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%

#Office 365

Sind Office 365 und Windows 10 sicher?

Ende-zu-Ende Schutz auch in Windows 10 EDU

- 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

#Office 365

Einwände von Datenschutzbehörden

Einwände von Datenschutzbehörden

Jüngste Diskussion, Behauptung: Microsoft sammelt für Office Telemetriedaten, ohne den Nutzer zu informieren und verletzt damit die DSGVO.

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
- Einer Einladung Microsofts vor einiger Zeit sind nur wenige gefolgt und haben bis heute keine gemeinsame Stellungnahme abgegeben

Einwände von Datenschutzbehörden

- 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://news.microsoft.com/de-de/datenschutz-microsoft/
- Microsoft aktualisiert auch laufend die Installationsroutinen, um die Transparenz in Bezug auf die Telemetriedaten so schnell wie möglich sicherzustellen und Wahlmöglichkeiten anzubieten.

Beispiel:

- Im April 2019 hat sich die niederländische (+dänische) Datenschutzbehörde bei Microsoft beschwert wegen der Telemetriedaten für Office. Microsoft hat diese Einwände beantwortet und
- Im Juli 2019 hat die NL Datenschutzbehörde veröffentlicht, dass sie nunmehr explizit Office 365 und Windows 10 empfiehlt: https://blogs.microsoft.com/eupolicy/2019/07/02/how-microsoft-works-with-customers-to-keep-their-trust-a-story-from-the-netherlands/

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

Situation in Bayern: Schulen

BayEUG Art. 85 Verarbeitung personenbezogener Daten

Die Schulen dürfen die zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlichen Daten verarbeiten.

>> Rechtmäßigkeit der Verarbeitung folgt aus dem Bildungsauftrag der Schule

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

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.lda.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.

#Office 365

Wie setze ich Office 365 DSGVO-konform ein?

Nutzung der Microsoft Office 365 Cloud durch Bildungseinrichtungen

- 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 der EU 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 Verfahrensverzeichnisses des Verantwortlichen → Ein Muster von co.Tec können Sie hier downloaden.
- Damit kann Office 365 datenschutzkonform in der Schule eingesetzt werden.

Die Datenschutzgrundverordnung

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

IT Dienste

Wer darf einer Bildungseinrichtung IT Dienste anbieten, bei denen personenbezogene 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

#Office 365

Zusammenfassung

Zusammenfassung

- ✓ 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. 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 nur innerhalb der EU.
- ✓ Alle Nutzdaten sind server- und verbindungsseitig verschlüsselt und zusätzlich individuell Ende-zu-Ende verschlüsselbar.
- ✓ Für die Inhalte ist der Auftraggeber selbst verantwortlich.

#Thankyou

www.cotec.de

co.Tec GmbH | Traberhofstraße 12 | 83026 Rosenheim

info@cotec.de | Tel: 08031/26350