Nutzung der Microsoft 365 (früher Office 365) Cloud durch Bildungseinrichtungen

Wie muss unsere Schule konkret vorgehen, wenn sie Microsoft 365 für Zusammenarbeit und in der Lehre einsetzen will?

Jede Schule verfügt bereits über eine IT Infrastruktur mit Kommunikations- und Lernelementen, die schulgesetzlich vorgeschriebene und/oder von der Schule ausgewählte Plattformen enthält. In dieser Anleitung geht es um die zusätzliche Einführung der Lern- und Kommunikationsplattform Microsoft 365, mit dem Ziel, die bestehende Infrastruktur zu ergänzen, zu erweitern und auszubauen. Sie finden eine Zusammenfassung der folgenden Hinweise auch als Handreichung.

1. Als ersten Schritt zur Einführung von Microsoft 365 in der Schule sollten die Vertreter der Bildungseinrichtung (Schüler, Lehrer, Eltern, Schulleitung) gemeinsam einen dementsprechenden Beschluss fassen. Hier finden Sie ein Muster für eine Beschlussvorlage. Nach erfolgtem Beschluss kann eine kondensierte Form als Datenschutzerklärung genutzt werden.
   Die rechtliche Grundlage zur Verarbeitung personenbezogener Daten in Microsoft 365 ergibt sich dann aus dem angestrebten Einsatzszenario:

2. **Optional: Microsoft 365 soll (zunächst) nur für Lehrkräfte eingeführt werden.**
   Als rechtliche Grundlage kann in diesem Fall Art. 6 Abs.1 lit c und e DSGVO in Verbindung mit dem Paragraphen über die Verarbeitung personenbezogener Daten aus dem Schulgesetz des Bundeslandes sein. Dies gilt sowohl für öffentliche als auch für private Schulen. Hier finden Sie ein Muster für den erforderlichen Eintrag in das Verzeichnis der Verarbeitungstätigkeiten.*
   Da es sich bei Microsoft 365 um eine technische Einrichtung handelt, die zur Leistungs- und Verhaltenskontrolle geeignet ist, unterliegt die Einführung der Mitbestimmung durch den Personalrat, insofern dieser vorhanden ist. Hier finden Sie eine Muster-Dienstvereinbarung zur Einführung von Microsoft 365.*

3. **Optional: Microsoft 365 soll für Lehrkräfte und Schüler eingeführt werden**, und das Schulgesetz ihres Bundeslandes verlangt die Vermittlung von Medienkompetenz und/oder den Einsatz von Lernplattformen. In diesem Fall wäre als rechtliche Grundlage der Art. 6 Abs.1 lit e DSGVO in Verbindung mit dem entsprechenden Paragraphen aus dem Schulgesetz anzuführen und Sie müssen das Verzeichnis der Verarbeitungstätigkeiten entsprechend anpassen. Beachten Sie bitte, dass keine Einwilligungen erforderlich sind, diese würden dem zitierten Art. 6 DSGVO widersprechen.*

   Die Beteiligungsrechte des Personalrates werden hierdurch nicht berührt. Die obige Muster-Dienstvereinbarung kann auch hier als Vorlage dienen.*
   Microsoft 365 soll für Lehrkräfte und Schüler eingeführt werden, im Schulgesetz ihres Bundeslandes ist der Einsatz einer Lernplattform o.ä. nicht verankert. Auch dann können Sie wie unter Punkt 1 ff beschrieben verfahren, als rechtliche Grundlage dient Art. 6 Abs.1 lit c und e DSGVO.

   Nach Meinung aller deutschen Landesdatenschutzbehörden muss eine Schule für jede IT-gestützte Lernplattform mit Beteiligung der Schüler zwingend auch eine Datenschutzfolgeabschätzung nach Art. 35 Abs. 3 anfertigen. Hier finden Sie eine Muster-Datenschutzfolgeabschätzung für den Einsatz von Microsoft 365.*

4. **Optional:** Soll **Microsoft 365 zuerst in einem Testbetrieb erprobt werden**, so ist dies am sinnvollsten mit der Einwilligung der Beteiligten.
   Hier finden Sie zwei Muster-Einwilligungen Muster-a und Muster-b. Wenn Schüler an diesem Pilotbetrieb beteiligt sind, so ist deren Einwilligung nur möglich, wenn sie 16 Jahre oder älter sind. Ansonsten ist eine Einwilligung der Erziehungsberechtigten notwendig.*

5. Schließlich haben Sie für die Schüler vermutlich bereits eine **Nutzungsordnung** für Internet-Nutzung, die Sie um die Microsoft 365 Dienste ergänzen sollten. Ein Muster finden Sie hier.*

*)Die dargestellten Vorgehensweisen und Beispieldokumente dienen lediglich dem unverbindlichen Informationszweck und stellen keine Rechtsberatung dar. Der Inhalt dieses Angebots kann und soll eine individuelle und verbindliche Rechtsberatung, die auf Ihre spezifische Situation eingeht, nicht ersetzen. Die Informationen wurden nach bestem Wissen und mit der gebotenen Sorgfalt zusammengestellt. Trotzdem kann keine Gewähr auf Richtigkeit oder Vollständigkeit gegeben werden.

Stellungnahme Schulministerium NRW: https://www.schulministerium.nrw/fragen-und-antworten-zum-datenschutz: Bereits seit mehreren Jahren bestehen länderübergreifende Prüfverfahren der Landesdatenschutzbehörden, eine abschließende umfassende Bewertung liegt nicht vor. Seitens des MSB wird daher weiterhin auf die datenschutzrechtlichen Bedenken gegen die Nutzung von MS 365-Produkten hingewiesen. Das MSB empfiehlt, bei der Beschaffung und Nutzung von cloudbasierten Anwendungen auf das landesseitig zur Verfügung gestellte Angebot LOGINEO NRW für Datenspeicherung und E-Mail-Verkehr, auf LOGINEO NRW LMS als Lernmanagementsystem sowie auf LOGINEO NRW Messenger mit integrierter Videokonferenzoption zurückzugreifen. Zudem ist künftig für LOGINEO NRW die Anbindung einer Office-Komponente vorgesehen. Andererseits ist zu berücksichtigen, dass es sich bei der Produktfamilie MS 365 um in Wirtschaft und Verwaltung weit verbreitete Anwendungen handelt. Insofern ist zu berücksichtigen, dass der Bildungs- und Erziehungsauftrag von Schule (§ 2 SchulG) auch den Aspekt des digitalen Kompetenzerwerbs beinhaltet, um für ein Studium und für berufliche Handlungsfähigkeit in einer digitalisierten Welt zu befähigen. Zudem waren bzw. sind einzelne Anwendungen, trotz offener datenschutzrechtlicher Fragestellungen, zur Organisation und Durchführung z.B. von digital erteiltem Distanzunterricht vielfach unumgänglich. Insoweit ist die Verpflichtung leitend, den - verfassungsmäßigen - Anspruch der Kinder und Jugendlichen auf Bildung erfüllen zu können; im Kern handelt es sich also um eine Grundrechtsabwägung. **Aus Sicht des MSB ist somit insgesamt ein generelles Verbot der Verwendung von MS-Produkten weiterhin derzeit nicht angezeigt**

Microsoft Stellungnahme: „Sind Microsoft 365 und Microsoft Teams datenschutzkonform? Die Antwort lautet „Ja!“ –
Können Microsoft 365 und Microsoft Teams in Unternehmen und im öffentlichen Sektor – insbesondere im Bildungsbereich – datenschutzkonform eingesetzt werden? Fragen wie diese sind oftmals Gegenstand von Debatten. Die Antwort lautet eindeutig ja. Warum unsere Produkte datenschutzkonform sind, warum Diagnosedaten in unseren Produkten und Services zum Einsatz kommen und was es mit dem Datentransfer in Drittstaaten auf sich hat, beantworten wir in diesem Paper. **https://news.microsoft.com/de-de/sind-microsoft-365-und-microsoft-teams-datenschutzkonform-die-antwort-lautet-ja/**

Zitat aus der Pressemitteilung des LfDI vom 25.04.2022:
„Bis zu den Sommerferien 2022 muss dann auf eine Alternative umgestiegen und die Nutzung von MS 365 bzw. MS Teams durch die Schule unterbunden sein, **sofern die datenschutzrechtlichen Mängel nicht eindeutig nachweisbar behoben wurden.**“

Microsoft Stellungnahme zu „Hinweise des LfDI zur Nutzung von Microsoft 365 durch Schulen“ vom 25. April 2022
"Wir haben die Pressemitteilung des LfDI zur Kenntnis genommen, die sich auf eine Bewertung aus dem April 2021 bezieht. Wir sind weiterhin fest davon überzeugt, dass Microsoft 365 auch an Schulen DSGVO-konform eingesetzt werden kann. Hierzu setzen wir die Gespräche mit Dr. Stefan Brink, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, fort um zu erläutern, wie die bisherigen Kritikpunkte aus dem Abschlussbericht behoben wurden und wie Schulen Microsoft 365 datenschutzkonform einsetzen können."

Dürfen Bildungseinrichtungen Microsoft 365 dienstlich und für den Unterricht einsetzen?
Ja, grundsätzlich dürfen Bildungseinrichtungen die Unternehmens-Plattform Microsoft-365 einsetzen, sofern sie dabei die Datenschutzgrundverordnung einhalten. Es ist wichtig zu verstehen, dass die Datenschutzverantwortung für jeden IT-Dienst, den die Bildungseinrichtung einsetzt, zur Gänze bei der Bildungseinrichtung liegt, nicht bei Microsoft. Bildlich gesprochen bietet Microsoft ein Fahrzeug an, das nach StVO alle Vorschriften erfüllt und zugelassen ist, aber der Fahrer ist die Bildungseinrichtung. Sie muss festlegen, warum welche personenbezogene Daten verarbeitet und gespeichert werden, wie lange sie gespeichert bleiben und wer Zugriff auf die Daten hat.
Außer den datenschutzrechtlichen Fragen, auf die wir in den folgenden Abschnitten noch detailiert eingehen, muss eine Bildungseinrichtung auch die Barrierefreiheit bei der Auswahl einer Lernplattform berücksichtigen (Behindertengleichstellungsgesetz, Barrierefreien-Informationstechnik-Verordnung § 3 Absatz 1 bis 4 und § 4 BITV 2.0). Dies bedeutet für eine Lern- und Kommunikationssoftware konkret, dass (1) dass sich die Benutzer geschriebenen Text und Bildmaterial vorlesen lassen können, (2) dass die Benutzer Texte durch Spracheingabe erstellen können, (3) Lernende mit Leseschwierigkeiten Texte vergrößert und zeilenweise darstellen können, (4) beim Unterricht mit digitalen Medien Live-Untertitel angezeigt werden können, (5) Live-Übersetzungen von Texten in den gängigen Sprachen zugänglich sind. Microsoft 365 erfüllt diese Anforderungen vollinhaltlich.
Wie stehen deutsche Landes-Schulbehörden zu Microsoft 365? Nach einer langen Zeit der Ablehnung oder übergangsweisen Duldung während der Pandemie hat das Ministerium für Schule und Bildung von Nordrhein-Westfalen im Februar 2023 Microsoft 365 im öffentlichen Interesse als zulässig bewertet, siehe hier und hier. Die Datenschutz-Bestimmungen für Schulen in NRW beschränken die Nutzung von Microsoft 365 weder mittels Einwilligung noch wird generell eine Datenschutzfolgeabschätzung als erforderlich betrachtet.

Welche gesetzlichen Grundlagen sind zu beachten, um Microsoft 365 in einer Bildungseinrichtung einsetzen zu dürfen?
Die Bildungseinrichtung (oder der Schulträger) schließt einen Auftragsverarbeitungsvertrag mit Microsoft Irland gemäß DSGVO ab. Dieser Vertrag besteht einmal aus den „Product Terms“, ergänzt durch den „Datenschutznachtrag zu den Produkten und Services von Microsoft“. Das DPA beinhaltet im Abschnitt „Datenschutzbestimmungen“ genaue Angaben über die Verarbeitung von Daten, die Pflichten von Microsoft sowie Details über getroffene Sicherheitsmaßnahmen. Zudem schließt Microsoft die sog. Standardvertragsklauseln ab, die sicherstellen, dass sowohl Microsoft Irland als auch Microsoft USA die europäischen Datenschutzrichtlinien vollinhaltlich erfüllt. Die Standardvertragsklauseln sind im Jahre 2010 erstmals von der EU-Kommission verabschiedet und sind aufgrund von Bedenken des EUGH am 04. Juni 2021 verschärft und von Microsoft in der neuen Form umgesetzt worden. Microsoft hat mittlerweile nicht nur die neuen, verschärften Standardvertragsklauseln implementiert, sondern ist deutlich darüber hinausgegangen und hat seine Vertragsklauseln noch einmal erweitert, um etwaige Vertragsverletzungen durch Behörden außerhalb der EU auszuschließen. Dies wurde auch von mehreren Landesdatenschutzbehörden (z. B. hier und hier) positiv bewertet.

Am 25. März 2022 hat die EU Kommission mit der US Regierung ein neues Datenschutzabkommen geschlossen, nach dem US Behörden grundsätzlich nur in sehr engem Rahmen Zugriff auf Daten von EU-Bürgern beantragen können, wobei die Betroffenen informiert werden und Rechtsmittel dagegen ergreifen können. Abgesehen davon, dass diese Fälle schon bisher extrem seltene Einzelfälle waren, würde Microsoft selbst diese Rechtsmittel auf eigene Kosten ergreifen.

Die Speicherung der Nutzdaten erfolgt nur innerhalb der EU. Microsoft Rechenzentren werden laufend nach strengsten internationalen Standards zertifiziert, sowohl nach ISO 27001, 27002, als auch nach dem Datenschutzstandard ISO 27018, ISO 27701 und dem höchsten deutschen Sicherheits-Standard BSI C5. Alle Nutzdaten sind server- und verbindungsseitig verschlüsselt. Die gespeicherten Daten können zusätzlich sehr einfach Ende-zu-Ende verschlüsselt werden (PurView Information Protection). Für die Inhalte ist der Auftraggeber selbst verantwortlich.

Eine ausführliche und aktuelle Darlegung der datenschutzrechtlichen Grundlagen zum legitimen Einsatz von Microsoft 365, in der auch immer wieder geäußerte Fragen und Bedenken angesprochen werden, finden Sie in diesem Compendium, das von der Rechtsabteilung von Microsoft Deutschland erstellt wurde. Zusätzliche Darlegungen zu den datenschutzrechtlichen Grundlagen bzgl. des Einsatzes von Microsoft 365 finden Sie hier. Verwechseln Sie bitte niemals die Firmen- und Organisations-Cloud Microsoft 365 mit den Privatkundenangeboten von Microsoft. Letztere sind nicht geeignet für den Einsatz in einer Bildungseinrichtung.

Was macht Microsoft mit Ihren Daten?

- Das Microsoft Geschäftsmodell basiert nicht auf der Kommerzialisierung von Kundendaten. Microsoft wird Kundendaten niemals für Werbezwecke oder ähnliche kommerzielle Zwecke nutzen.
- Grundlage des Vertragverhältnisses zwischen der Bildungseinrichtung und Microsoft ist der Auftragsverarbeitungsvertrag Microsoft Online Services Terms, ergänzt durch den Anhang zu den Datenschutzbestimmungen für Onlinedienste, der auch die neuen, wegen dem sog. Schrems II Urteil des EUGH verschärften Standardvertragsklauseln als Vertragsbestandteil enthält.
  Bildungseinrichtungen können nach einem kürzlichen Urteil des Oberlandesgerichts Karlsruhe darauf vertrauen, wenn ihnen ein IT-Anbieter Datenschutz-Kompatibilität zusichert, wie dies für Microsoft 365 der Fall ist. Das abstrakte Risiko eines Zugriffs von Stellen außerhalb der EU alleine ist nach dem Urteil kein Verbotsgrund mehr.
- Art 35 der DSGVO gibt vor, dass eine Datenschutzfolgeabschätzung (DSFA) durchzuführen ist, wenn Daten von schutzbedürftigen Personen betroffen sind. Das Ergebnis einer DSFA lässt sich kurz in einer Risikomatrix zusammenfassen, in der die Eintrittswahrscheinlichkeit einer Verletzung der DSGVO gegen die Auswirkung aus Sicht der Betroffenen dargestellt wird.
  Wir haben sehr sorgfältig eine solche DSFA für die Plattform Microsoft 365 erstellt, mit dem Ergebnis, dass für keinen schulrelevanten Aspekt von Microsoft 365 ein erhöhtes Risiko besteht. Schulen können diese DSFA als Muster für die eigene Datenschutzfolgeabschätzung einsetzen. Kürzlich hat eine Anwaltskanzlei ebenfalls eine Muster-DSFA für Schulen kostenlos online gestellt.
- Microsoft ermöglicht dem Nutzer von Microsoft 365 eine sehr komfortable Ende-zu-Ende Verschlüsselung (PurView Information Protection), die deutlich über ältere Methoden wie S/MIME oder PGP hinausgeht. Es ist insbesondere auch möglich, Teams-Besprechungen mit hochsensiblen Daten in besonderer Weise zu schützen , u. z. durch Ende-zu-Ende Verschlüsselung sowohl der Chats als auch aller Besprechungsdaten und zusätzlich durch sog. Vertraulichkeitsbeziehungen, die festlegen, welche Kommunikationsmittel ein- oder ausgeschaltet sind.
- Die Daten in den EU Rechenzentren sind in mehreren Ebenen verschlüsselt.
- Die Nutzerdaten werden ausschließlich in der EU gespeichert.
- Der Datentransfer zu Microsoft 365 und zwischen den Microsoft Rechenzentren ist verbindungstechnisch verschlüsselt. Zusätzlich werden alle Daten innerhalb der Rechenzentren durchgängig verschlüsselt gespeichert.
- Microsoft hat per 01.01.2023 das EU Datengrenzen-Programm ins Leben gerufen. Dieses Programm hat zum Ziel, dass sämtliche personenbezogene Daten nicht nur (wie schon bisher) in der EU gespeichert, sondern auch zur Gänze in der EU verarbeitet werden. Phase 1 ist bereits in Kraft und betrifft alle Kundendaten und Dokumentation, Phase 2 (bis Ende 23) betrifft pseudonymisierte Daten in systemerzeugten Logdateien, und in Phase 3 (bis Ende 24) umfasst es auch technische Supportdaten. Phase 2 betrifft nur Bildungseinrichtungen, die Teams-Festnetz-Telefonie einsetzen und Phase 3 lässt sich schon jetzt durch die sog. Kunden-Lockbox kontrollieren. Nur Maßnahmen zum Schutz vor komplexen modernen Sicherheitsbedrohungen werden nach wie vor weltweit verarbeitet, denn Hacker agieren weltweit und die DSGVO verlangt den Schutz personenbezogener Daten nach Stand der Technik. Dies betrifft z. B. das Erkennen eines kompromittierten Benutzers (durch gleichzeitige Anmeldung des Nutzers aus Deutschland und aus Übersee) oder Erkennen von Datenexfiltration. Diese Schutzmaßnahmen stehen mit den Produkten Microsoft 365 Defender und Microsoft Cloud Security zur Verfügung.
- Seit Februar 2023 gibt es nun eine detaillierte Übersicht über die Diagnosedaten für Office (Microsoft 365 Apps for Enterprise). Es gibt drei Ebenen von Diagnosedaten für die Office-Clientsoftware, aus denen Sie wählen können: Erforderlich, Optional, oder Weder noch. In letzterem Falle werden keine Diagnosedaten an Microsoft gesendet. Auch wenn keine Diagnosedaten gesendet werden, müssen aber zumindest erforderliche Dienstdaten vom Gerät an Microsoft gesendet werden, wie z. B. die Lizenzierung der Produkte oder Ihre Wahl der Zustimmung. Da Datenschutzbehörden immer wieder behaupten, Microsoft würde nicht alle Details für die Kategorie "Wesentliche Dienste für Office" und "Erforderliche Diagnosedaten" offenlegen, hat Microsoft nunmehr auf fast 1000 Seiten eine bis ins letzte Detail gehende Aufstellung publiziert, die erstere Daten und letztere Daten auflistet.
- Ebenfalls seit Februar 2023 beschreibt Microsoft auf über 4000 Seiten in dem von den Datenschutzbehörden verlangten Detailgrad die Teams-Technologie und sämtliche mit Teams zusammenhängende Diagnosedaten. Es gibt wie bei Office drei Ebenen von Diagnosedaten für die Teams-Software, aus denen Sie wählen können: Erforderlich, Optional, oder Weder noch. Keine dieser Diagnosedaten enthalten Namen von Benutzern, ihre E-Mail-Adressen oder andere Benutzerinhalte. Welche Daten bei der Wahl "Erforderlich" übermittelt werden, ist hier beschrieben.

Behauptung: man darf keine Daten in der "Cloud" speichern
Fakt: Daten in Microsoft 365 können durchgängig Ende-zu-Ende verschlüsselt gespeichert werden (Azure Information Protection) und der Zugriff kann auf einfache Art und Weise nur berechtigten Personen der Bildungeinrichtung ermöglicht werden. Damit sind die Daten in Microsoft 365 wesentlich besser geschützt als auf lokalen Servern. In der DSGVO kommt es nicht auf den Speicherort an, sondern nur darauf, dass personenbezogene Daten nachweislich nach Stand der Technik geschützt werden. Es ist daher nicht verwunderlich, dass auch die Bundesregierung Microsoft 365 für die Datenspeicherung einsetzt.

Behauptung: Microsoft (Support-)Mitarbeiter außerhalb der EU haben Zugriff auf personenbezogene Daten
Fakt: der Zugriff auf personenbezogene Daten durch Supportmitarbeiter außerhalb der EU kann grundsätzlich unterbunden werden (sog. Lockbox).

Behauptung: es ist unklar, wo die Daten liegen
Fakt: der aktuelle Speicherort wird für alle Services in Microsoft 365 in der administrativen Konsole explizit angezeigt.

Behauptung: Microsoft gibt Nutzerdaten an die US-Regierung weiter
Fakt: Dies entbehrt jeder sachlichen Grundlage. Es gab vor Jahren den sog. Patriot-Act, der US Regierungsbehörden in gewissen Fällen Zugriff auf Daten ermöglicht hätte, aber dieses Gesetz ist aufgrund der Veröffentlichungen durch Snowden abgeschafft worden. Microsoft publiziert im Gegenteil im Trustcenter in großer Ausführlichkeit, welche Daten von welchen Behörden weltweit - auch aus Deutschland! - verlangt werden und wie Microsoft rechtskonform damit umgeht.

Behauptung: Microsoft transferiert Daten außerhalb der EU im Rahmen des Privacy Shields, was vom EUGH gekippt wurde
Fakt: Microsoft speichert Nutzdaten ausschließlich innerhalb der EU und transferiert keine Daten im Rahmen des Privacy Shields. Es gibt mehrere Möglichkeiten, Datentransfers in die USA zu legitimieren, insbesondere EU-Standardvertragsklauseln, die nach dem Urteil des EUGH gültig bleiben. Die Standardvertragsklauseln sind fester Bestandteil des Auftragsverarbeitungs-Vertrags, den Microsoft anbietet und der sich über alle Microsoft 365-Dienste erstreckt. Hier finden Sie eine ausführliche Stellungnahme von Microsoft zum grenzüberschreitenden Datentransfer, die auf das EUGH Urteil eingeht. Um einen noch höheren Schutz der Benutzerdaten zu garantieren und auf Einwände des EUGH einzugehen, hat Microsoft kürzlich seine Vertragsklauseln noch einmal erweitert, was von einigen Landesdatenschutzbehörden auch sehr positiv beurteilt wurde.

Behauptung: der Cloud-Act ermöglicht US-Behörden einseitig Zugriff auf Daten von EU-Bürgern
Fakt: USA hat den sog. Cloud-Act beschlossen. Das ist ein Gesetz, welches das Recht eines Gerichts regelt, Daten im Rahmen eines Strafverfahrens z. B. von Microsoft oder einer anderen Firma in der Welt direkt zu erbitten statt über ein Rechtshilfeverfahren, das Jahre dauert und nicht mehr zeitgemäß ist. Es ist ausgelegt als bilaterales Abkommen und schon von einigen Ländern wie Großbritannien unterzeichnet worden. Es geht dabei um normale Gerichtsverfahren. In dem extrem unwahrscheinlichen Fall, dass ein Europäer in USA in ein Strafverfahren verwickelt ist und dieses Gericht von Microsoft Daten dieses Straftäters haben will, die noch dazu in der EU liegen, würde Microsoft erstens den Angeklagten informieren und für ihn ggf. in seinem Auftrag Widerspruch einlegen. Mehr dazu finden Sie hier.

Behauptung: Die von Microsoft beauftragten Unterauftragsverarbeiter bleiben im Dunkel
Fakt: Microsoft veröffentlicht die Namen neuer Unterauftragsverarbeiter für zentrale Onlinedienste mindestens sechs Monate vor ihrer Autorisierung zur Ausführung von Diensten, die ggf. Zugriff auf Kundendaten erfordern. Microsoft veröffentlicht die Namen neuer Unterauftragsverarbeiter für personenbezogene Daten mindestens 14 Tage vor ihrer Autorisierung zur Ausführung von Diensten, die ggf. Zugriff auf solche Daten erfordern. Die vollständigen Listen aller Unterauftragsverarbeiter sind unter diesem Link verfügbar.

Behauptung: Microsoft sammelt Telemetriedaten, ohne den Nutzer zu informieren und verletzt damit die DSGVO
Fakt: Alle großen Software-Anbieter übertragen bei der Nutzung ihrer Software anonymisierte Daten an den Hersteller. Dies hat zwei Gründe. Grund Nr. 1 ist Funktionskontrolle und mögliche Verbesserung: funktionieren die Dienste wie beabsichtigt? Sind sie gut nutzbar? Wo treten Probleme auf? Grund Nr. 2 ist die Analyse der Hardware, Treiber, Software-Versionen usw., um Sicherheitsschwächen beheben und Aktualisierungen vorzunehmen zu können. Diagnosedaten werden von Microsoft nicht für Werbung, Profilbildung oder Nutzer-Tracking eingesetzt. Microsoft dokumentiert auf seinen öffentlichen Webseiten im Detail, welche Daten aus Windows, Office, dem Edge-Browser und weiteren Diensten zu Microsoft übertragen werden: Browserdaten, Office Daten, Office Einstellungen, Windows 10 Daten, Windows 10 Einstellungen.
Darüberhinaus gibt es den kostenlosen Diagnosedatenanzeiger, mit der Sie als Anwender alle Diagnosedaten, die in Windows 10 und Microsoft 365 gesammelt werden, analysieren und kontrollieren können. Dies ist vor kurzem für Windows 10 Education (Seite 22 dieses Links) von der bayerischen Datenschutzbehörde bestätigt worden. Viele Telemetriedaten sind notwendig, damit Microsoft den entsprechenden Softwareliefervertrag erfüllen kann. Dafür ist nach DSGVO keine Einwilligung erforderlich, sondern nur eine Information darüber, wie in den obigen Links angeführt. Trotzdem gibt es immer wieder Diskussionen über die Legitimität der Telemetriedaten. So hat der Heise-Verlag vor einigen Monaten eine entsprechende Beschwerde der niederländischen Datenschutzbehörde zum Datenschutz-GAU hochstilisiert, obwohl die niederländische Behörde kurze Zeit später aufgrund der Anpassungen von Microsoft eine sehr positive Bilanz und Empfehlung für Microsoft 365 Apps und Windows 10 ausgesprochen hat. Diese Prozesse erfordern immer einen Kompromiss zwischen Transparenz und Wahlmöglichkeiten einerseits und praktischer Benutzbarkeit und Sicherheit der Software andererseits und werden daher auch immer Anpassungen erfordern.
Man findet in diesem Zusammenhang immer wieder Vorschläge, beispielsweise das "Customer Experience Improvement Program in den Microsoft 365 Apps" zu deaktivieren. Die anerkannte Qualität von Microsoft Office beruht aber ganz zentral auf den vielen Rückmeldungen und Vorschlägen der weltweiten Benutzer. Wir raten ausdrücklich davon ab, solchen Empfehlungen zu folgen. Es wäre sehr bedauerlich, wenn sich der europäische Konsument dadurch zum stimmlosen und unmündigen Nutzer degradieren ließe oder, weit schlimmer, unwissentlich sicherheitsrelevante Eigenschaften abschaltet.

Behauptung: Mängel bei Videokonferenzdienst Teams und im Auftragsverarbeitungsvertrag
Fakt: Die Berliner Datenschutzbehörde kritisiert in einer Publikation vom Juni 2020, dass die Identität der Teilnehmenden an einer Teams-Konferenz nicht gesichert sei und es viele Mängel im Auftragsverarbeitungsvertrag (AVV) gäbe. Tatsache ist, dass der Teams-Administrator in Microsoft 365 anonyme Konferenzteilnahme, Gästezugriff und externen Zugriff ein- oder ausschalten kann und die Identität durch Mehrfaktor-Anmeldung gesichert ist. Die behaupteten Mängel im AVV hat Microsoft Deutschland in einer Stellungnahme ausführlich entkräftet.

Behauptung: Konferenz der unabhängigen Datenschutzaufsichtsbehörden behauptet "mehrheitlich", dass kein datenschutzgerechter Einsatz von Microsoft 365 möglich sei.
Fakt: Diese Behauptung enthält weder konkrete, noch aktuelle Bewertungen der in Microsoft 365 enthaltenen Dienste, noch wurde Microsoft Deutschland eingebunden oder um Klärung gebeten. Bedauerlicherweise muss man feststellen, dass einige Datenschutzaufsichtsbehörden in Deutschland offensichtlich gar kein Interesse an Fakten haben, wie aus der Pressemitteilung deutlich wird. Die Glaubwürdigkeit einiger Datenschutzaufsichtsbehörden wurde durch diesen Artikel beschädigt. Eine Rechtsanwältin für Datenschutz aus Hamburg hat dazu einen sachgerechten Artikel verfasst. Die Diskrepanz zwischen sachfremden Argumenten und einer ernsthaften Beschäftigung mit dem Thema Microsoft 365 zeigt besonders deutlich die jüngste Veröffentlichung der Landesdatenschutzbehörde von Baden-Württemberg.

Worum geht es bei der DSGVO?
Dieses Gesetz regelt ausschließlich die automatisierte Verarbeitung von personenbezogenen Daten, also Daten, mit denen sich ein eindeutiger Bezug zu einer Person herstellen lässt. Es geht also nicht um den Schutz geistigen Eigentums. Die Kernidee ist, dass es für die Verarbeitung personenbezogener Daten einen vernünftigen, schlüssigen Grund geben muss und die Betroffenen das Recht haben, zu erfahren, wer, wozu, wo und wie lange diese Daten gespeichert werden.

Was sind die Kernaussagen der neuen DSGVO gegenüber dem alten Bundesdatenschutzgesetz?
Es sind im Zusammenhang mit dem Einsatz von IT in Bildungseinrichtungen insbesondere die folgenden drei Aussagen, die vollkommen neu und relevant sind:
Artikel 1 (3) der DSGVO lautet: „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“. Daher ist eine Beschränkung auf Deutschland oder eine Beschränkung auf die eigenen Räumlichkeiten nicht zulässig. Damit spielt erstmals das "wo" keine Rolle, sondern nur das "wie".
Sie müssen als Bildungseinrichtung nach Artikel 32 DSGVO belegbar Auskunft geben können, welche Maßnahmen in technischer und organisatorischer Hinsicht getroffen wurden, um die Datenschutzbestimmungen einzuhalten. Die technischen Schutzmaßnahmen müssen „dem aktuellen Stand der Technik“ entsprechen, was für lokal betriebene Server in kaum einer Bildungseinrichtung gewährleistet werden kann. Diese Forderung bedeutet eine vollkommene Abkehr vom bisherigen Prinzip „my home is my castle“, das in dem 30 Jahre alten Bundesdatenschutzgesetz vertreten wurde, weil es vor dem Internetzeitalter verfasst wurde.
Das Gesetz setzt sich erstmals mit den dramatisch wachsenden Gefahren durch technische Sicherheitslücken auseinander und verlangt den technisch bestmöglichen Schutz personenbezogener Daten in Abhängigkeit von den Nachteilen, die einer Person durch unbeabsichtigte Veröffentlichung entstehen können. Im Kern anerkennt die DSGVO damit, dass angesichts der Entwicklung des Internets ein adäquater Datenschutz durch eine lokale Serverinfrastruktur in aller Regel nicht mehr erbracht werden kann. Nur sehr große, professionell betriebene und entsprechend ausgestattete Rechenzentren verfügen über die Mittel, den wachsenden Bedrohungen wirksame Schutzmaßnahmen entgegensetzen zu können. Dies wiederholt in gewissen Sinne die Jahrzehnte alte Entwicklung in einem anderen Bereich: weg vom Kohle- oder Ölofen in jeder Wohnung hin zur heutigen Fernwärme. Niemand wird heute den dadurch erreichten Sicherheitsgewinn mehr bestreiten.

Wer darf einer Bildungseinrichtung IT Dienste anbieten, bei denen personenbezogene Daten verarbeitet werden?
Für die Auswahl von IT Dienstleistern („Auftragsverarbeiter“) gelten in der DSGVO wesentlich strengere Maßstäbe und eine Bildungseinrichtung muss konkret nachweisen können, dass die Auswahl nach objektiven datenschutzrechtlichen Kriterien erfolgt ist, z. B. durch eine Zertifizierung des Anbieters. So sind z. B. die Microsoft EU Rechenzentren nach dem Datenschutz-Standard ISO 27018 zertifiziert. Artikel 28 (1) lautet: „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt …“.

Sind außer der DSGVO noch weitere datenschutzrechtlich relevante Gesetze von Bildungseinrichtungen zu beachten?
Im Gegensatz zu früher gilt die DSGVO für öffentliche und nicht öffentliche Organisationen gleichermaßen und sie ist das relevante Gesetz, das stets Vorrang gegenüber anderen Gesetzen zum Datenschutz hat. Die DSGVO sieht allerdings Öffnungsklauseln für den öffentlichen Dienst vor und das neue Bundesdatenschutzgesetz (BDSG-neu) und einige neuen Landesdatenschutzgesetze nutzen diese zur Regelung von Gefahrenabwehr (z. B. mittels Videoüberwachung), Strafverfolgung und -vollzug und für Datenverarbeitung im Beschäftigungskontext. Relevant sind diese Öffnungsklauseln für öffentliche Bildungseinrichtungen noch in einem weiteren kleinen Teilaspekt, weil sie danach von der Verhängung von Geldbußen befreit sind.
Für eine Bildungseinrichtung gibt es außerdem Schul- bzw. Hochschulgesetze, die datenschutzrechtliche Aspekte enthalten können. So sieht zum Beispiel das Bayerische Erziehungs- und Unterrichtsgesetz ein Verbot der Erfassung von Schülerdaten zwecks Werbung in der Schule vor.

Darf meine Bildungseinrichtung personenbezogene Daten auf freiwilliger Basis verarbeiten?
Ja, allerdings nur, wenn die Betroffenen nachweislich über alle Umstände und Risiken aufgeklärt wurden und die Zustimmung wirklich freiwillig erfolgt. Die DSGVO versteht freiwillig im Sinne von "unerheblich", also Dinge, auf die man auch verzichten kann, ohne dadurch einem gewissen sozialen Druck ausgesetzt zu sein. Für Kinder unter 16 Jahren ist eine Zustimmung aller Erziehungsberechtigten empfehlenswert, aber für Unterrichtszwecke nicht zwingend vorgeschrieben.

Welche Services bietet co.Tec an?

- Tenantinspektion oder Remoteservicevertrag:
  - Wir schauen uns Ihren Tenant gemeinsam an und behandeln Datenschutzrelevante Themen.
  - Tenanteinstellungen werden überprüft und ggf. gemeinsam gelöst.
  - Nötige Mustervorlagen werden zur Verfügung gestellt.

- Alternativ: co.Tec Shopservice – Wir übernehmen die Datenschutzverantwortung für den Tenant. Völlige Anonymisierung der Konten. Microsoft 365 Apps for Enterprise (Office) als Downloadversion. Es handelt sich hier um einen freiwilligen Kauf für Lehrer und Schüler: