

Datenschutzkonzept, Datenschutzfolgenabschätzung & Formulare

zur Nutzung von Microsoft 365 an den Schulen in Oberlenningen
Lenningen, Juni 2025

Die europäische Datenschutzgrundverordnung regelt 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 Zugriff auf die Daten hat?
- Warum der Zugriff besteht?
- Wo die Daten verarbeitet werden?
- Wie lange eine Verarbeitung erfolgt?

Wichtige Eckpunkte der DSGVO

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".

Eine Bildungseinrichtung ist nach Artikel 32 DSGVO verpflichtet, darüber Auskunft geben zu können, welche Maßnahmen in technischer und organisatorischer Hinsicht getroffen wurden, um die Datenschutzbestimmungen einzuhalten. Die technischen Schutzmaßnahmen müssen „dem aktuellen Stand der Technik“ entsprechen.

Das Gesetz setzt sich 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 deren 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 oft 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.

Verarbeitung im Auftrag

Wenn eine Bildungseinrichtung ihre IT nicht mehr selbst betreiben will oder soll, wer ist dann verantwortlich? Es ist wichtig zu verstehen, dass die Datenschutzverantwortung bei jedem IT-Dienst, den die Bildungseinrichtung einsetzt, zur Gänze bei der Bildungseinrichtung liegt, nicht beim Kultusministerium, nicht beim Schulträger, und auch nicht beim Auftragsverarbeiter wie z. B. einem Unternehmen wie Microsoft. Die Bildungseinrichtung muss festlegen, warum welche personenbezogenen Daten verarbeitet und gespeichert werden, wie lange sie gespeichert bleiben und wer Zugriff auf die Daten hat.

Für die Auswahl von IT-Dienstleistern (Auftragsverarbeiter nach Art. 28 DSGVO) 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 die Microsoft EU Rechenzentren nach dem Datenschutz-Standards ISO 27001 und 27018 (<https://aka.ms/compliance-angebote>) 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 ...“.

Welche Gesetze sind im Zusammenhang mit IT zu beachten?

Grundsätzlich gibt es eine Gesetzes-Hierarchie: EU-Recht wie die DSGVO geht vor Bundesrecht geht vor Landesrecht. Bei Konflikten gilt das Gesetz der übergeordneten Instanz, untergeordnete Gesetze regeln Dinge, die im übergeordneten nicht geregelt sind.

Die DSGVO gilt für öffentliche und nicht öffentliche Organisationen gleichermaßen und ist das relevante Gesetz für alle datenschutzrechtlichen Aspekte. Die DSGVO sieht allerdings Öffnungsklauseln für den öffentlichen Dienst vor. Das neue Bundesdatenschutzgesetz und die neuen Landesdatenschutzgesetze nutzen diese zur Regelung von Gefahrenabwehr (z. B. mittels Videoüberwachung), Strafverfolgung und -vollzug und Dienstvereinbarungen. Relevant sind diese Öffnungsklauseln für öffentliche Bildungseinrichtungen in einem kleinen Teilaspekt auch deswegen, weil sie danach von der Verhängung von Geldbußen befreit werden.

Für eine Bildungseinrichtung gibt es außerdem die Schul- bzw. Hochschulgesetze, die datenschutzrechtliche Aspekte enthalten können wie z. B. ein generelles Werbeverbot an Schulen. Alle Landes-Schulgesetze enthalten Absätze, in denen die Verarbeitung personenbezogener Daten zum Zwecke der Erfüllung der schulischen Aufgaben geregelt ist. Auf dieses Recht zur Verarbeitung personenbezogener Daten in Schulen, das im öffentlichen Interesse liegt, bezieht sich auch die DSGVO.

Einsatz von IT gestütztem Unterricht

Eine staatlich anerkannte Bildungseinrichtung hat den gesetzlichen Auftrag, Lernenden eine zeitgemäße Ausbildung anzubieten. Dazu gehört in allen Fällen eine Bewertung der Leistungen des Lernenden und in vielen Fällen (wie z. B. in etlichen Schulgesetzen verankert ist) die Vermittlung moderner Medienkompetenz.

Das Bundesministerium für Bildung und Forschung beschreibt: „Digitalisierung prägt mittlerweile unsere Lebenswelt. Die nötigen digitalen Kompetenzen sollen in der Schule vermittelt werden. Das erfordert eine bessere Ausstattung der Schulen. Mit dem DigitalPakt Schule wollen Bund und Länder dieses Ziel erreichen.“

Vermittlung von Medienkompetenz und die Digitalisierung sind nicht ohne Weiteres mit der DSGVO verträglich. Andererseits muss jede Verarbeitung personenbezogener Daten rechtmäßig sein. Es muss also eine Rechtsgrundlage für die Verarbeitung von Personendaten vorliegen. Daher ist eine wichtige Frage, wie eine Schule IT-gestützten Unterricht datenschutzkonform anbieten kann. Kurz gesagt, gibt es 2 Möglichkeiten: man kann IT-gestützten Unterricht freiwillig, also auf Basis einer Einwilligung laut DSGVO, anbieten oder nach einem Beschluss des Schulgremiums, dem alle Gruppen einer Schule (Lehrer-, Schüler-, Eltern-Vertreter) angehören.

Freiwilliger Einsatz ist sinnvoll, wenn es um eine Pilotgruppe geht oder einen Testlauf. Der springende Punkt bei freiwilligem Einsatz ist, dass ein Betroffener jederzeit seine Einwilligung widerrufen kann. Nach einem solchen Widerruf ist zu überlegen, ob der Testlauf noch fortgesetzt werden kann, denn ein sozialer Druck auf die Teilnehmer darf dadurch nicht entstehen.

Für systematischen Einsatz von IT-gestützten Unterricht ist aber ein Beschluss zu empfehlen, den wir weiter unten erläutern und eine entsprechende Vorlage vorhalten.

Der Einsatz von Microsoft 365 im Schulalltag

An Microsoft scheiden sich, zumindest in Deutschland, die Geister. Dass Microsoft in Sachen Cybersecurity sehr stark aufgestellt ist, zweifelt vermutlich niemand an. Entsprechend ist es für Microsoft auch unproblematisch entsprechende ISO/IEC Standards einzuhalten und die dazugehörigen Zertifizierungen zu erhalten bis einschließlich dies C5 Testats des BSI.

Wir als Schulen haben gute Gründe die Nutzung von Microsoft 365 vorzusehen. In der heutigen digitalen Welt ist es wichtig, dass Schüler Zugang zu den neuesten Technologien haben, um sich optimal auf ihr Berufsleben vorzubereiten. Eine der am häufigsten genutzten Plattformen in diesem Bereich ist Microsoft 365. Es gibt mehrere Gründe, warum es sich lohnt, sich mit dem Einsatz von Microsoft 365 auseinanderzusetzen. Diese erläutern wir im nächsten Abschnitt „Verhältnismäßigkeit und Notwendigkeit“.

Nachstehend soll in diesem Konzept eine Lösung gefunden werden, wie Microsoft 365 so datenschutzkonform wie möglich an Schulen in Lenningen betrieben werden kann. Hierzu führen wir zuerst transparent eine seitens der DSGVO vorgesehene Datenschutzfolgenabschätzung mit ihren

Unterpunkten durch, beleuchten dann alle seitens der DSGVO geforderten Elemente für den Einsatz von Microsoft 365 und liefern am Ende des Konzepts Vorlagen, die zwingend für den datenschutzkonformen Einsatz von Microsoft 365 genutzt werden sollen.

Datenschutzfolgenabschätzung Microsoft 365

1. Verhältnismäßigkeit und Notwendigkeit

Die Zwecke der Verarbeitung von Daten mithilfe von Office 365 werden vom Datenverantwortlichen bestimmt, der die Anwendung implementiert, konfiguriert und verwendet. Wie in den Microsoft Online Services-Nutzungsbedingungen und den Hinweisen zum Datenschutz angegeben, verarbeitet Microsoft als Datenverarbeiter Personendaten, um Nutzern die Onlinedienste entsprechend ihren dokumentierten Anweisungen bereitzustellen.

Microsoft ist für die Verarbeitung personenbezogener Daten verantwortlich, um diese spezifischen legitimen Geschäftsvorgänge zu unterstützen. Im Allgemeinen aggregiert Microsoft personenbezogene Daten, bevor diese für deren Geschäftsvorgänge verwendet werden, wobei die Möglichkeit zur Identifizierung bestimmter Personen durch Microsoft entfernt wird. Die personenbezogenen Daten werden in der am wenigsten identifizierbaren Form verwendet, die die für Geschäftsvorgänge erforderliche Verarbeitung unterstützt.

Microsoft verwendet Personendaten oder daraus abgeleitete Informationen nicht für Profilerstellungs- oder Werbezwecke oder ähnliche kommerzielle Zwecke.

Alternative Verfahrensmöglichkeiten anstelle von Microsoft sind denkbar. Als mögliche Alternative zu Microsoft 365 an Schulen verweist der Landesdatenschutzbeauftragte in Baden-Württemberg auf die Lernplattformen Moodle oder Itslearning, welche den Schulen vom Kultusministerium kostenlos angeboten werden. Über die Integration von Big Blue Button könnten zudem Videokonferenzen durchgeführt werden. Allerdings kommen diese Tools für uns Schulen nicht in Frage, weil sie die oben genannten Vorzüge von Microsoft-Produkten nicht abbilden.

Einer der wichtigsten Gründe gegen die Nutzung der vom Landesdatenschutzbeauftragten vorgeschlagenen „Insellösungen“ ist der gemeinsame Datenspeicher (Cloud), der es ermöglicht, dass Schüler überall – ob iPad, Schulrechner oder PC – die gleichen Zugangsdaten haben und auf die gleiche Datenbasis zugreifen können. Dies vereinfacht den Datenaustausch und die Zusammenarbeit unter Schülern und Lehrern erheblich.

Ein weiterer wichtiger Faktor ist die Einfachheit, die durch eine einheitliche Plattform und keine Insellösungen und verschiedenen Tools entsteht. Dies ermöglicht ein einheitliches Bedienkonzept und eine bessere Usability für Videokonferenzen, Datenversand und Kalender. Schüler und Lehrer können sich schneller zurechtfinden und effizienter miteinander arbeiten.

Eltern und Lehrer spielen eine wichtige Rolle bei der Entscheidung für eine bestimmte Plattform. Wir als Schule haben die Erfahrung gemacht, dass viele Eltern möchten, dass ihre Kinder Microsoft 365 nutzen, um sich auf das Berufsleben vorzubereiten.

Ein letzter wichtiger Grund ist die Vorbereitung der Schüler auf das Berufsleben. Indem Schüler Microsoft 365 nutzen, lernen sie die gleiche Plattform kennen, die auch in vielen Unternehmen und Organisationen verwendet wird. Sie erwerben damit wertvolle Fähigkeiten und Kenntnisse, die ihnen im Berufsleben von großem Nutzen sein werden.

Insgesamt bietet der Einsatz von Microsoft 365 viele Vorteile für Schüler und Lehrer. Es ermöglicht eine einfachere Zusammenarbeit, eine bessere Usability und vor allem eine bessere Vorbereitung der Schüler auf das Berufsleben. Daher lohnt es sich, sich genauer mit dieser Plattform auseinanderzusetzen.

2. Beschränkung der Datenverarbeitung auf das notwendige Maß

Folgende Kategorien von Daten werden laut Microsoft verwendet:

- Nutzerdaten: dabei handelt es sich um alle Daten, einschließlich Text-, Ton-, Video- oder Bilddateien und Software, die Microsoft von den Schulen durch die Nutzung der Services bereitgestellt werden. Darunter fallen auch Daten, die Nutzer zum Speichern oder zur Verarbeitung hochladen, sowie auch Anpassungen. Beispiele für in Office 365 verarbeitete Kundendaten

umfassen E-Mail-Inhalte in Exchange Online sowie Dokumente oder Dateien, die in SharePoint Online oder OneDrive für Unternehmen gespeichert sind.

- Vom Dienst generierte Daten: Dies sind Daten, die von Microsoft durch den Betrieb des Diensts generiert oder abgeleitet wurden, wie z.B. Nutzungs- oder Leistungsdaten. Die meisten dieser Daten enthalten pseudonyme Bezeichner, die von Microsoft generiert werden.
- Diagnosedaten: Diese Daten werden von Microsoft gesammelt oder aus einer Software abgerufen, die vom Kunden in Verbindung mit dem Onlinedienst lokal installiert wurde. Diese Daten werden auch als Telemetriedaten bezeichnet. Sie werden häufig durch Attribute der lokal installierten Software oder des Computers, auf dem die Software ausgeführt wird, identifiziert.
- Unterstützungsdaten: Diese Daten sind von oder im Namen der Schulen an Microsoft bereitgestellt z.B. durch einen Kontakt mit Microsoft, um technischen Support für Onlinedienste zu erhalten.

Kundendaten, vom System generierte Protokolldaten und Unterstützungsdaten umfassen keine Administrator- und Abrechnungsdaten, z. B. Kontaktinformationen für den Kundenadministrator, Abonnementinformationen und Zahlungsdaten, die Microsoft in seiner Rolle als Datenverantwortlicher erfasst und verarbeitet.

3. Korrektheit der Daten und deren Aufbewahrung

Der Nutzer hat die Möglichkeit, die erhobenen Daten in seinem Microsoft-Account bzw. der IT-Administrator in der Microsoft365-Adminconsole aktuell zu halten.

Wie in den Datenschutzbedingungen der Online Services-Nutzungsbedingungen dargelegt, speichert Microsoft Kundendaten für die Dauer der Nutzung des Diensts durch den Nutzer und bis zu dem Zeitpunkt, an dem alle Nutzerdaten gelöscht oder gemäß den Kundenanweisungen oder den Online Services-Nutzungsbedingungen zurückgegeben wurden.

Während der Laufzeit des Abonnements hat die Schule zu jedem Zeitpunkt Zugriff auf die Kundendaten, die in dem Dienst gespeichert sind, und kann diese extrahieren und löschen, wobei in manchen Fällen eine bestimmte Produktfunktionalität zum Tragen kommt, die das Risiko eines versehentlichen Löschens minimieren soll (z. B. den Exchange-Ordner für wiederhergestellte Elemente). Dies ist in der Produktdokumentation im Detail beschrieben.

Microsoft speichert solche Daten, die in den Onlinediensten gespeichert sind, 90 Tage nach Ablauf oder Kündigung des Abonnements der Schule auf einem eingeschränkten Konto, sodass der Kunde die Daten extrahieren kann. Nach der 90-tägigen Speicherfrist deaktiviert Microsoft das Konto und löscht die Daten.

Im Falle von vom System generierte Daten werden diese standardmäßig bis zu 180 Tage nach Erfassung gespeichert; längere Aufbewahrungszeiträume sind möglich, wenn dies zur Sicherheit der Dienste oder zur Erfüllung rechtlicher oder behördlicher Vorschriften erforderlich ist.

Für personenbezogene Daten aus dem Europäischen Wirtschaftsraum, der Schweiz und dem Vereinigten Königreich stellt Microsoft sicher, dass die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation den entsprechenden Bestimmungen gemäß Artikel 46 der DSGVO unterliegt. Ist der entsprechende Service aktiviert, überträgt Microsoft die Daten nicht in ein Drittland.

Zusätzlich zu Microsofts Verpflichtungen unter den Standardvertragsklauseln für Auftragsverarbeiter und anderen Musterverträgen hält sich Microsoft weiterhin an die Bedingungen des EU-US-Datenschutzschild-Frameworks, wird sich aber nicht mehr darauf als Grundlage für die Übermittlung personenbezogener Daten aus der EU/dem EWR in die Vereinigten Staaten stützen.

4. Maßnahmen zum Schutz der Persönlichkeitsrechte

Nutzer werden mit Hilfe einer Datenschutzhinweise über die Verarbeitung ihrer Daten in Microsoft 365 informiert. Es ist keine Einwilligung nötig, um die Daten in Microsoft 365 zu verarbeiten, da ein Beschluss der Schulkonferenz vorliegt. Die Rechtsgrundlage der Verarbeitung ist Art. 6, Abs. 1, lit. c) und e) DSGVO.

Gegenüber dem Verantwortlichen können Betroffene ihre Rechte unter der E-Mail-Adresse ausüben: schulleitung@04123341.schule.bwl.de. Welche Rechte bestehen, ist der Datenschutzerklärung im Anhang zu entnehmen.

Wenn bei Microsoft ein Antrag einer betroffenen Person oder einen der Schulen erhält, die von einem oder mehreren ihrer Rechte Gebrauch machen möchte, bittet Microsoft die betroffene Person, ihren Antrag direkt an den Datenverantwortlichen zu stellen.

Microsoft fasst personenbezogene Daten in der Regel zusammen, bevor sie für die Geschäftsvorgänge verwendet werden, und ist nicht in der Lage, in dem Aggregat personenbezogene Daten für eine bestimmte Person zu identifizieren. Dies reduziert das Datenschutzrisiko für den Einzelnen erheblich. Wenn Microsoft nicht in der Lage ist, die Person zu identifizieren, kann es die Rechte der betroffenen Person auf Zugriff, Löschung, Übertragbarkeit oder die Einschränkung oder Ablehnung der Verarbeitung nicht unterstützen.

5. Verpflichtungen einer Auftragsverarbeitung

Wenn Office 365 Education als Plattform zum Einsatz kommt, tritt Microsoft hier als Auftragsverarbeiter gemäß Art. 28 DSGVO auf. Der entsprechende Auftragsverarbeitungsvertrag heißt Microsoft Online Services Terms und wurde im Januar 2020 durch den Anhang zu den Datenschutzbestimmungen für Onlinedienste ergänzt, der auch die Standardvertragsklauseln als Vertragsbestandteil enthält und mit der EU-Datenschutzbehörde abgestimmt wurde.

Des Weiteren ist wichtig, dass Microsoft für den Betrieb weitere Unterauftragsverarbeiter in Anspruch nimmt. Eine Liste dieser liegt hier vor (<https://aka.ms/uav>).

6. Übertragung der Daten in Drittländer

Stellungnahmen öffentlicher Stellen, insbesondere die einiger Datenschutzbehörden, erwecken bereits seit längerem möglicherweise den Eindruck, Microsoft 365 und Microsoft Teams für Unternehmen und die öffentliche Hand (insb. den Bildungssektor) könnten nicht datenschutzkonform eingesetzt werden oder seien gar selbst nicht datenschutzkonform.

Aus Sicht von Microsoft und der Sicht von uns als Schulen bietet Microsoft zukunftsweisende Technologien mit branchenführendem Sicherheitsstandard, auf die Deutschland sich auch in Krisenzeiten verlassen kann. Nur konsequente Digitalisierung mit Technik auf dem Stand der Zeit wird es Deutschland ermöglichen, seinen Wohlstand zu wahren, seine Werte zu verteidigen und seinen gesellschaftlichen Aufgaben erfolgreich nachzukommen (etwa dem Bildungsauftrag).

Wir sehen Microsoft als einen zuverlässigen Partner, dessen Geschäftsmodell darin besteht, durch Technologie zum Erfolg seiner Kunden beizutragen. Dabei sind wir der Überzeugung, dass Microsoft Produkte und Dienste in der Privatwirtschaft und im öffentlichen Sektor (z.B. an Schulen) datenschutzkonform eingesetzt werden können. Microsoft hält unserer Ansicht nach die Anforderungen des geltenden Datenschutzrechts ein.

Microsoft bietet uns vertragliche Zusagen und technische Mittel, um Microsoft Produkte und Dienste datenschutzkonform nutzen zu können, insbesondere:

- Schuldaten nicht für sachfremde Zwecke wie Werbung verwendet;
- rechtliche Schutzmaßnahmen gegen unrechtmäßige Herausgabeverlangen von Behörden oder Dritten ergreift;
- Dritten, wenn überhaupt, nur im vertraglich vorgesehenen Umfang Zugriff auf Kundendaten gewährt;
- für die Verschlüsselung von Kundendaten verwendete Plattform-Schlüssel nicht preisgibt und Dritten auch nicht die Möglichkeit einräumt, die Verschlüsselung zu überwinden; und
- keinen Grund zur Annahme hat, durch anwendbare Gesetze an der Einhaltung der Verpflichtungen unter den Standardvertragsklauseln gehindert zu sein; und
- Möglichkeiten zur technischen Absicherung von Daten (z.B. Verschlüsselung, Pseudonymisierung, differenzierte Zugriffsberechtigungen und die Automatisierung von sicherheitsrelevanten Prozessen) nach dem aktuellen Stand der Technik.

Microsoft speichert Daten weitgehend regional in Rechenzentren in der EU. Zusätzlich – obwohl es keine gesetzliche Verpflichtung dazu gibt – wird die Microsoft EU Data Boundary es künftig in der EU ansässigen

Kunden aus dem öffentlichen Sektor und Unternehmenskunden ermöglichen, ihre Daten innerhalb der EU zu verarbeiten und zu speichern.

Microsoft ist im Bereich der Cyber Security führend und hat eine Vielzahl technischer Maßnahmen implementiert, um Kundendaten vor Cyberattacken zu schützen. Hierzu gehören unter anderem Technologien zur Erkennung und Vereitelung von Attacken und unberechtigten Datenzugriffen. Microsoft unterzieht sich mindestens einmal im Jahr Überprüfungen von international anerkannten unabhängigen Auditoren. Diese überprüfen auf Grundlage des ISO/IEC 27001-Standards, ob Microsoft die Richtlinien und Verfahren für Sicherheit, Datenschutz, Kontinuität und Konformität gewährleistet. Weiterhin erfüllt Microsoft den Anforderungskatalog Cloud Computing (C5) des BSI6 und verfügt über eine Vielzahl weiterer relevanter Zertifizierungen und Attestierungen wie z.B. den ISO/IEC 27018-Standard für Datenschutz in der Cloud und den ISO/IEC 27701-Standard zum Datenschutz-Risikomanagement.

Risikoszenarien

Risikoszenarien beziehen sich auf mögliche Bedrohungen für die Sicherheit von Daten und Systemen. Einige häufige Risikoszenarien sind der unrechtmäßige Zugriff auf Daten, welcher sich darauf bezieht, dass unbefugte Personen Zugriff auf geschützte Daten oder Systeme erlangen, z.B. durch Hacken oder Phishing.

Ein weiteres Szenario ist die unerwünschte Veränderung von Daten. Hierbei handelt es sich um unbeabsichtigte oder absichtliche Änderungen an Daten oder Systemen, die zu Fehlern oder Problemen führen können. Das letzte Szenario, das wir im Rahmen unserer Risikoüberlegungen zu Microsoft 365 betrachten wollen ist ein potenzieller Datenverlust. Dieser kann durch menschliches Versagen, technische Fehler oder Angriffe verursacht werden und bezieht sich darauf, dass Daten unwiederbringlich verloren gehen oder unbrauchbar gemacht werden.

Im Folgenden sollen die Szenarien im Hinblick auf die konkrete Nutzung von Microsoft 365 stichpunktartig betrachtet werden.

1. Unrechtmäßiger Zugriff

Was können die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

- Kontrollverlust über die eigenen Daten
- Aufhebung der Pseudonymisierung und Verlust der Vertraulichkeit
- Verletzung von Berufsgeheimnissen

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

- Verfälschungen bzw. Zerstörungen bei Übertragungen
- Datenverluste bzw. Zerstörungen bei Übertragungen
- Angriffe aus dem Internet, Verfälschungen, Verschlüsselung etc.
- Spionage
- Verluste bzw. Schäden bei Dienstleistern

Was sind die Risikoquellen?

- Externe menschliche Risikoquelle
- Computerviren
- Technischer Fehler

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei? (siehe nächstes Kapitel)

- Passwort-Richtlinie
- Bildschirmsperre
- Umgang mit E-Mails
- Schulungen

Wie wird der Risikoschweregrad beim Eintritt eines Risikoszenarios eingeschätzt? → überschaubar

Wie wird die Eintrittswahrscheinlichkeit eines Risikoszenarios eingeschätzt? → unwahrscheinlich

2. Unerwünschte Veränderung

Was können die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

- Kontrollverlust über die eigenen Daten
- Finanzieller Verlust
- Verletzung von Berufsgeheimnissen

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

- Angriffe aus dem Internet, Verfälschungen, Verschlüsselung etc.
- Verfälschungen bzw. Zerstörungen bei Übertragungen
- Verwendung nicht getesteter und nicht freigegebener Programme

Was sind die Risikoquellen?

- Technischer Fehler
- Interne menschliche Risikoquelle
- Externe menschliche Risikoquelle
- Computerviren

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei? (siehe nächstes Kapitel)

- Datenschutz-Management
- Passwort-Richtlinie
- Bildschirmsperrung
- Firewall
- Virenschutz
- Umgang mit E-Mails
- Backup- und Recoverykonzept

Wie wird der Risikoschweregrad beim Eintritt eines Risikoszenarios eingeschätzt? → überschaubar

Wie wird die Eintrittswahrscheinlichkeit eines Risikoszenarios eingeschätzt? → entfernt vorstellbar

3. Datenverlust

Was können die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

- Finanzieller Verlust
- Verletzung von Berufsgeheimnissen
- Rufschädigung

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

- Sabotage
- Angriffe aus dem Internet, Verfälschungen, Verschlüsselung etc.

Was sind die Risikoquellen?

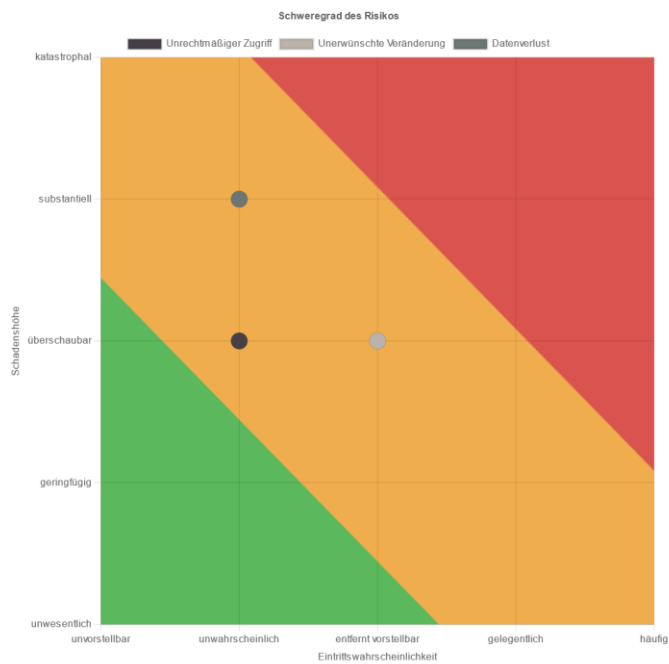
- Interne menschliche Risikoquelle
- Externe menschliche Risikoquelle
- Technischer Fehler
- Computerviren

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei? (siehe nächstes Kapitel)

- Firewall
- Virenschutz
- Umgang mit E-Mails
- Backup- und Recovery-Konzept

Wie wird der Risikoschweregrad beim Eintritt eines Risikoszenarios eingeschätzt? → substanziell

Wie wird die Eintrittswahrscheinlichkeit eines Risikoszenarios eingeschätzt? → unwahrscheinlich



Technische und organisatorische Maßnahmen (TOMs)

Risiken lassen sich niemals vollständig ausschließen, sondern können lediglich minimiert werden. Dies bedeutet, dass es immer ein gewisses Restrisiko gibt, das nicht vollständig vermieden werden kann.

Es ist wichtig, die potenziellen Risiken, die bestehenden Schutzmaßnahmen und die Möglichkeiten zur Risikominderung zu erkennen und zu verstehen. Eine gründliche Analyse und Identifizierung von Risiken ist der erste Schritt, um das Risiko erfolgreich zu minimieren. Diese Analyse ist mit der Darstellung der Szenarien gerade erfolgt.

Um den dargestellten Risikoszenarien zu begegnen und Risiken weitestgehend zu minimieren, stellen wir hier geplante bzw. bestehende TOMs dar, die wir als Schulen aber auch Microsoft selbst ergreifen.

Richtigstellungen seitens Microsoft

In seiner Stellungnahme aus August 2022 entgegnet Microsoft diversen Annahmen, die in Bezug auf die Nutzung der Anwendungen in Schulen kursieren.

Diese möchten wir hier kurz nach dem Prinzip der Nennung der Annahmen und der Richtigstellung durch Microsoft im Folgenden, darstellen.

„Die Cloud ist unsicher.“

Die Cloud-Nutzung führt zu einer erhöhten Sicherheit und Verfügbarkeit von Daten im Vergleich zu On-Premise-Lösungen. Der aktuelle Krieg in der Ukraine zeigt, dass Länder, die eine Cloud-Strategie verfolgen, weniger von Cyber-Angriffen betroffen sind.⁹

Vorschriften zum technologischen Schutz von Daten (z.B. Art. 32 DS-GVO) machen es erforderlich, den Schutz an die technischen Gegebenheiten fortwährend anzupassen und weiterzuentwickeln. Cloud-Lösungen bilden fortlaufend die aktuellen Sicherheitsanforderungen ab.

- „Die US-Regierung liest alles mit.“

Ein Interesse von US-Behörden z.B. an Daten aus einem Schulunterricht in Deutschland kann nicht ernsthaft behauptet werden.

Eine umfangreiche Auswertung öffentlich verfügbarer Dokumente von US-Regierungs-Behörden zur Nutzung von §702 des Foreign Intelligence Surveillance Act (FISA) in der Praxis¹⁰ belegt dagegen:

Es gibt keinen Anhaltspunkt dafür, dass die US-Regierung §702 FISA nutzt, um Industriespionage zu betreiben oder US-amerikanische wirtschaftliche Interessen zu verfolgen oder Regierungen im Europäischen Wirtschaftsraum ins Visier zu nehmen; und

Die US-Regierung nutzt §702 FISA im Wesentlichen zur Sammlung von Informationen für Ermittlungen zu schwerwiegenden Bedrohungen der nationalen Sicherheit, wie Terrorismus, Cyber Security-Angriffe und Waffenproliferation.

Microsoft hat die US-Regierung mehrmals erfolgreich verklagt, um die Datenschutz-Rechte seiner Kunden zu verteidigen.¹¹ Microsoft bezieht auch weiterhin Stellung, um Kundendaten zu verteidigen.

Microsofts „Transparency Reporting“ zeigt, dass eine erzwungene Herausgabe von außerhalb der USA befindlicher Unternehmensdaten an amerikanische Strafverfolgungsbehörden in nur sehr wenigen Fällen erfolgt ist.

Die pauschale Empfehlung seitens einzelner Behörden, nur Anbieter aus der EU zu nutzen, verkennt im Übrigen, dass auch Anbieter mit Stammsitz innerhalb der EU US-Überwachungsgesetzen unterliegen können, z.B. durch eine Präsenz in oder minimalen Kontakt mit den USA. Behörden dürfen nicht mit zweierlei Maß messen und unterliegen dem Objektivitätsgebot.

- „Datentransfers in Drittstaaten wie die USA sind unzulässig.“

Die DS-GVO erlaubt Übermittlungen in Drittstaaten, einschließlich in die USA, unter Nutzung von geeigneten Garantien (z.B. Standardvertragsklauseln 2021/914 und zusätzliche Maßnahmen).

Dabei ist eine Risikoanalyse im Lichte der Schrems II-Rechtsprechung des EuGH durchzuführen und es sind ggf. zusätzliche Maßnahmen zu implementieren.

Microsoft bietet für Datenübermittlungen in Drittstaaten zusätzliche, rechtlich anerkannte Schutzmechanismen, wie zusätzliche vertragliche Klauseln.

Es ist rechtlich nicht geboten, jedes theoretische Restrisiko, etwa eines behördlichen Zugriffs im Drittstaat, im Zusammenhang mit einer internationalen Datenübermittlung auszuschließen.¹⁴ Einen „Null-Risiko-Ansatz“ zu fordern, ist unverhältnismäßig und steht weder im Einklang mit der DS-GVO noch mit den Regelungen der Standardvertragsklauseln¹⁵, der Schrems II-Rechtsprechung und den Empfehlungen des Europäischen Datenschutzausschusses für Maßnahmen zu Datenübermittlungen in Drittstaaten.

- „Diagnosedaten sind nicht notwendig und schädlich.“

Diagnosedaten sind notwendig, um Produkte und Dienste sicher und stabil zu betreiben. Unsere Kunden erwarten zurecht, dass sie unsere Produkte und Dienste vertragsgemäß und sicher nutzen können. Die verantwortungsvolle Nutzung von Diagnosedaten trägt dazu bei.

Kunden nutzen viele verschiedene technische Infrastrukturen. Die Verarbeitung von Diagnosedaten ist daher sehr nützlich, um die Anfälligkeit für Fehler und die Wahrscheinlichkeit von Sicherheitsrisiken zu verringern.

Diagnosedaten werden oft falsch verstanden und mit Funktionsdaten verwechselt, z.B., weil entsprechende (Fehl-)Einordnungen außer Acht lassen, dass für die vertraglich vereinbarte und daher vom Kunden auch zurecht erwartete Stabilität und Sicherheit der jeweiligen Anwendung (und damit für deren ordnungsgemäßes Funktionieren) bestimmte Daten erfasst werden müssen, um die gewünschte Aktion des Nutzers auszuführen.

- „Microsoft überwacht die Nutzer seiner Produkte und Dienste.“

Die technische Verbindung zwischen Nutzer und Microsoft (z.B. über Server und Rechenzentren) ist in vielen Fällen zwingende Voraussetzung für die vertraglich geschuldete Dienstleistung. Nichts davon kann als ein Ausspähen von Kunden angesehen werden.

Cloud-Dienste funktionieren nur, wenn Nutzeraktionen übermittelt werden, damit die jeweilige Reaktion der Applikation ausgeführt werden kann (z.B. eine Übersetzung). Das ist technisch mit Verarbeitungen bei On-Premise-Lösungen vergleichbar.

- „Einen Dienst darf nur einsetzen, wer die technische Funktionsweise des Diensts voll versteht.“

Eine Analyse jedes einzelnen Prozesses eines Diensts durch den Verantwortlichen/Nutzer ist datenschutzrechtlich weder erforderlich noch geboten und geht weit über die Rechenschaftspflichten unter Art. 5 (2) DS-GVO hinaus. Entscheidend ist, dass die verantwortliche Stelle die notwendigen Informationen besitzt, um seinen Rechenschaftspflichten nachzukommen.

Das Errichten einer solchen Hürde würde das Ende vieler Hyperscaling Technologien im Cloud-Umfeld bedeuten, denen ein Wissensgefälle zwischen dem Anbieter der Technologie und dem Nutzer inhärent ist. Dies zu fordern wäre unrealistisch und technologiefeindlich. Entsprechende Anforderungen können in kaum einem maßgeblich von Technik beeinflussten Lebensbereich eingehalten werden.

Es ist anerkannt, dass die reine technische Umsetzung durch den Auftragsverarbeiter selbst in gewissem Rahmen bestimmt werden kann

Eigene TOMs – bestehende Sicherheitsmaßnahmen

Trotz der aus unserer Sicht guten Sicherheitsmaßnahmen, die Microsoft ins Leben gerufen hat und auch den Schulen anbietet, haben wir weitere eigene Schutzmaßnahmen ins Leben gerufen, die wir als Schulen ergreifen, um das datenschutzrechtliche Risiko der Nutzung von Microsoft zu minimieren.

- Datenschutzmanagement

Es besteht ein schulinternes Datenschutz-Management, dessen Einhaltung ständig überwacht sowie anlassbezogenen und mindestens halbjährlichen evaluiert wird.

- Wahrung der Betroffenenrechte

Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

- Passwort-Richtlinie

Die Profil- und Kennwortangaben sind geheim zu halten und dürfen keiner dritten Person zur Verfügung gestellt werden. Auch sind Hinweise auf diese Angaben am Arbeitsplatz oder am Arbeitsplatzcomputer zu unterlassen. Für die erstmalige Anmeldung am System wird ein Initialkennwort zugeteilt. Dieses gilt nur für eine Anmeldung und muss dann sofort geändert werden. Passwörter dürfen nicht mit anderen geteilt werden. Zur Speicherung der Passwörter ist ein Passwort-Safe zu nutzen. Kennwörter sind so zu wählen, dass sie nach menschlichem Ermessen weder leicht zu erraten noch leicht ausprobiert werden können.

Es gelten folgende Kennwortregeln: Mindestlänge 8 Zeichen bestehend aus Buchstaben, Zahlen, Groß- und Kleinschreibung und Sonderzeichen (z.B.: # ! & ?).

- Bildschirmspernung

Alle Mitarbeitenden sind über die Datenschutzrichtlinie aufgefordert, beim Verlassen des Arbeitsplatzes ihren Bildschirm zu sperren.

- Firewall & Virenschutz

Außerhalb der Nutzung der Tablets in der Grundstufe im SBBZ existieren in jeder Schule eine Firewall und ein Virenschutz.

- Umgang mit E-Mails

Die Nutzer von Microsoft 365 wurden insgesamt zum Umgang mit dem Versand und dem Empfang von E-Mails sensibilisiert.

- Backup- und Recoverykonzept

Es existiert ein ständig kontrolliertes Sicherungs- und Wiederherstellungskonzept, das von Microsoft im Standard gestellt wird.

- Benutzerverwaltung

Die Online-Lernplattform ist so zu konfigurieren, dass ausschließlich die zur pädagogischen Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.

Bei der Benutzerverwaltung durch den Administrator ist zwischen dem Anzeigenamen und dem Anmeldenamen zu unterscheiden. Der Anzeigename kann den Klarnamen (Vor-/Nachname) des Benutzers enthalten. Der Klarname ist zur Identifikation des Schülers durch Lehrer und Schüler erforderlich und muss nicht dem Anmeldenamen entsprechen. Der Anmelde-name (Teil der E-Mail-Adresse) wird bei der Anmeldung im System verwendet und muss nicht mit dem Benutzernamen identisch sein. Die Nutzung von Pseudonymen als Anmeldenamen kann die Sicherheit im Vergleich zur Nutzung des Klarnamens erhöhen, erhöht aber auch die Komplexität der Nutzung.

Zumindest für die Lehrer und Verwaltung der Schule empfehlen wir, die in Office 365 integrierte und komfortable Möglichkeit der Zwei-Faktor-Anmeldung zu nutzen. Damit ist die Gefahr eines Identitätsdiebstahls stark vermindert. Office 365 bietet darüber hinaus eine sehr komfortable Möglichkeit, Daten und E-Mails zu verschlüsseln („Azure Information Protection“) und bietet einen wirksamen Schutz gegen komplexe Bedrohungen („Office 365 Advanced Threat Protection“).

Folgende Rollen sind in einer Online-Lernplattform in der Regel vorgegeben:

- Administrator: Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- Kursverwalter: Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- Lehrkraft: Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.
- Teilnehmer: Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

In Übereinstimmung mit dem Rollen- und Berechtigungskonzept der Schule können weitere Rollen definiert werden. Benutzerkonten von Schülern und Lehrern sind nach deren Ausscheiden aus der Schule zu löschen

- Weitere Konfiguration in Microsoft Office 365

Die datenschutzrechtliche Herausforderung liegt nun darin, die Details im Admin-Center so einzustellen, dass Microsoft 365 den Anforderungen der DSGVO genügt. Hier spielen die detaillierten Zugriff- und Compliance-Einstellungen eine Rolle, als auch Aspekte der Sicherheit wie Backup und Virenschutz. Nach dem Update auf eine aktuelle Version können folgende DSGVO-konformen Konfigurationen vorgenommen werden:

- Connected Experiences deaktivieren;
- Diagnosedaten deaktivieren;
- Telemetriedatenübertragung deaktivieren;
- Customer Lockbox verwenden;
- LinkedIn-Integration deaktivieren;
- Workplace-Analytics tendenziell deaktivieren bzw. im Detail Mitarbeiter informieren;
- Bei der Buchung des Produkts M365 ein Hosting auf Servern auf EU-Boden forcieren.

Stellungnahmen und Empfehlungen

Im August 2022 veröffentlichte Microsoft Deutschland eine Stellungnahme zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams. Mit der Stellungnahme reagiert Microsoft Deutschland auf die Stellungnahmen öffentlicher Stellen und von einigen Aufsichtsbehörden und möchte damit dem Eindruck, der daraus entstanden sein könnte, dass sowohl Microsoft 365 als auch MS Teams nicht datenschutzkonform im öffentlichen Sektor und im Bildungsbereich nutzbar seien, entgegenreten.

Dazu stellt man die Stärken von Microsoft in Bezug auf Datenschutz und -sicherheit heraus und widerlegt gängige Aussagen der Gegner von Microsoft Cloud Produkten (siehe oben). Es wird versichert, dass die genannten Dienste den Datenschutzrichtlinien entsprechen würden. Kurz zusammengefasst sind die wichtigsten Punkte:

- Alle Microsoft Produkte und Dienste entsprechen den geltenden Datenschutzrichtlinien und dürfen demnach auch im öffentlichen Sektor eingesetzt werden.

- Microsoft bietet vertragliche Zusagen sowie technische Mittel, um dessen Produkte und Dienste datenschutzkonform nutzen zu können.
- Daten werden weitgehend regional in Rechenzentren in der EU gespeichert. Künftig wird die Microsoft EU Data Boundary für weitere Sicherheiten sorgen.

Bewertung der Datenschutzkonformität

Microsoft speichert aktuell die Daten von Kunden „weitgehend regional in Rechenzentren in der EU“ und wird Kunden aus dem öffentlichen Sektor künftig anbieten, Daten ausschließlich innerhalb der EU nicht nur zu speichern, sondern auch zu verarbeiten. Damit liegen die Daten von EU-Kunden dann nicht mehr im unmittelbaren Zugriff von US-Behörden.

Leider besteht aber weiterhin die Zugriffsmöglichkeit im Rahmen des CLOUD-Acts. Und hier argumentiert Microsoft, nachvollziehbar, indem man aktuelle Veröffentlichungen, wie etwa die des LfDI Baden-Württemberg aufgreift, dass es nicht erforderlich ist, jegliches Restrisiko eines Zugriffs von US-Behörden auszuschließen.

Wie in einem Gutachten für die Datenschutzkonferenz und jüngst auch in einem niederländischen Memo beschrieben, unterliegen theoretisch auch EU-Unternehmen dem CLOUD-Act, wenn sie geschäftliche Beziehungen in die USA unterhalten. Dass Gegner einer Nutzung von Microsoft Cloud Produkten mit zweierlei Maß messen, wenn sie den CLOUD-Act nur im Zusammenhang mit der Nutzung von Microsoft Produkten kritisch sehen, nicht jedoch wenn es um EU-Unternehmen geht, die ebenfalls betroffen sein könnten, ist ein Argument, welches plausibel erscheint. Gleiches gilt auch für den Hinweis, dass die Anfragen von US-Ermittlungsbehörden Schulen nicht betreffen.

Microsoft sieht seine Cloud Produkte als datenschutzkonform nutzbar an deutschen Schulen. Der Anbieter tut tatsächlich eine Menge, um Schutz und Sicherheit der Daten zu gewährleisten.

Was tun wir als Schulen nun konkret?

Um Microsoft 365 Education in einer Bildungseinrichtung nutzen zu können müssen die durch die DSGVO geforderten Schritte eingehalten und dokumentiert werden:

- Positive Prüfung des Anbieters anhand offizieller Zertifizierung des Cloud-Anbieters gemäß Art. 42 DSGVO (ISO 27001, ISO 27018, BSI C5, Privacy Shield, etc.)
- Vorliegen eines Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO (AVV)
- Vorliegen einer Rechtsgrundlage gemäß Art. 6 DSGVO
- Vorliegen einer Verpflichtung gemäß Art. 6 Abs. 1 lit. c und e, Abs. 2 und 3 DSGVO im Verbund mit dem entsprechenden Absatz des Schulgesetzes und
- Beschluss der Schulkonferenz (Schulleitung, Personalrat, Schülerbeirat, Elternbeirat)
- Vorliegen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO (VVV)
- Vorliegen technischer und organisatorischer Maßnahmen gemäß Art. 25, 32 DSGVO (TOM)
- Vorliegen einer schulspezifischen Nutzungsordnung

Diese Dokumentationen wurden abgeschlossen, die entsprechenden Formulare an die Betroffenen ausgegeben. Vor diesem Hintergrund und vor dem Hintergrund der aufgeführten Technischen und Organisatorischen Maßnahmen ist die Verwendung von Microsoft 365 aus der Sicht von uns als Schulen der Gemeinde Lenningen mit einem überschaubaren datenschutzrechtlichen Risiko vertretbar.

Wichtig ist, dass die Schule immer die datenschutzrechtlich verantwortliche Stelle bleibt. Microsoft ist nur Dienstleister bzw. Auftragsverarbeiter. Somit muss die Schule die Rechtmäßigkeit der Verarbeitung sicherstellen. Des Weiteren ist die Schule für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen sowie der Betroffenenrechte verantwortlich bzw. zuständig.

Wir haben uns mit den von der DSGVO geforderten Themen intensiv auseinander gesetzt und stellen unseren Nutzern, nämlich Schülern, deren Eltern und Lehrkräften, Formulare zur Verfügung, die entsprechend informieren.

Folgende Formulare aus den Anhängen dieses Dokuments sind für den internen Gebrauch in den Schulen vorgesehen:

- Beschluss zum Einsatz der Lernplattform Office 365 an unserer Schule
- Technische und Organisatorische Maßnahmen (TOMs) für die Verwendung von Microsoft Office 365
- Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gem. Artikel 30 Abs. 1 DSGVO

Folgende Formulare aus den Anhängen dieses Dokuments sind für die Ausgabe an Schüler, Eltern und Lehrkräfte vorgesehen:

- Nutzungsordnung für das pädagogisches Netz
- Datenschutzerklärung zur Nutzung von Microsoft Office 365

Ihre Schulleitung

Theresa-Maria Breier

Anhang 1

Beschluss zum Einsatz der Lernplattform Office 365 an unserer Schule

Vorabbeurkundung Dienstvereinbarung für Lehrer und Lehrerinnen

Bevor Office 365 Education als Plattform genutzt werden kann, sollten alle relevanten Entscheidungsträger in die Entscheidungsfindung eingebunden werden:

- Schulleitung
- Lehrervertretung bzw. Personalrat in der Schule oder beim Schulamt
- Schüler- und Elternvertretung

Evtl. sollten der Datenschutzbeauftragte der Schule, Systembetreuer der Schule (auch Externe, wie z.B. ein Systemhaus oder IT-Partner) und Schulträger (Stadt oder Landkreis) eingebunden werden.

Bei den schulinternen Entscheidern (Schulleitung, Datenschutzbeauftragter, Systembetreuer, Schüler-/Elternvertretung) reicht meist eine Schulkonferenz aus, um einen Entschluss zu fassen.

Die Schulkonferenz als oberstes Mitwirkungs- bzw. Beschlussgremium an unserer Schule, in dem die Schulleitung, die Vertretung der Lehrer, Eltern und Schüler vertreten sind, fasst am 14.07.2025 in Übereinstimmung mit Bestimmungen der Schulordnungen und Lehrerdienstordnung, sowie Art. 6 Abs. 1 lit c und e der Datenschutzgrundverordnung den im Folgenden ausgeführten Beschluss.

Vorbemerkung: Wenn im Text aus Gründen der Lesbarkeit die männliche Form gewählt wird, gelten die Aussagen in gleicher Weise für Angehörige aller Geschlechter.

Gegenstand dieser Vereinbarung

Diese Vereinbarung dient der Unterstützung unserer Schule bei der Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben mit Hilfe von Microsoft Office365 zur Umsetzung des Bildungs- und Erziehungsauftrags, bei der Abwicklung der schulinternen Aufgaben und Abläufe und der Umsetzung der Medienkompetenzen im Rahmen der Digitalisierung.

Unsere Schule ist verpflichtet, unseren Schülern eine zeitgemäße Medienkompetenz zu vermitteln, die Schüler mit den vielfältigen Einsatzmöglichkeiten moderner Medien vertraut macht und Ihnen die Chancen und Risiken dieser neuen Technologien in ausgewogener Form nahebringt. Voraussetzung ist selbstverständlich, dass auch unsere Lehrerschaft mit denselben Technologien vertraut ist bzw. vertraut gemacht wird.

Eine grundlegende Anforderung dabei ist, dass die Schule die volle Kontrolle über Umfang, Art der Wissens-Vermittlung und Nutzung der Daten beim Einsatz von digitalen Lernplattformen behält. Es ist immer der Lehrer, der in jedem Fach und jeder Klasse in Absprache mit Schülern und Eltern entscheidet, in welcher Form Informationstechnologien den Unterricht sinnvoll ergänzen und bereichern können.

Konkretisierung dieser Vereinbarung

Wir schlagen nach sorgfältiger Analyse der Angebote am Markt vor, die Lernplattform Microsoft Office 365 als eine der digitalen Angebote in unserer Schule einzusetzen. Diese Vereinbarung ergänzt den bereits bestehenden Einsatz der bisherigen Lernplattformen und internetgestützten schulischen Angebote.

Name des eingesetzten Verfahrens und Dienstbeschreibungen

Microsoft Office 365 (<http://aka.ms/Wkcowi>)

<https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx>

Ort der Speicherung

Es ist vertraglich gesichert, dass alle Nutzdaten nur innerhalb der EU in den Rechenzentren von Microsoft (für deutsche Kunden liegen diese in Frankfurt und Berlin) gespeichert werden und von Microsoft in keiner Weise ausgewertet oder gelesen werden können.

Alle Daten werden verschlüsselt über das Internet übertragen und in den Rechenzentren von Microsoft maschinell verschlüsselt gespeichert. Zugriff auf die Nutzdaten hat nur die Schule und die von der Schule beauftragten Systembetreuer.

Art der gespeicherten Daten

Grundsätzlich sind die vorgegebenen Kontodaten in Office 365 keine besonders schutzwürdigen Daten, sondern nur solche, deren Verfügbarkeit innerhalb der Schule von den Betroffenen erwartet wird und das Minimum an Daten darstellt, das für die Erfüllung der Aufgaben des Einzelnen erforderlich ist.

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, E-Mailadresse, weitere dienstliche E-Mailadressen, Unterrichtsmaterialien, Schüleraufgaben, von den Benutzern selbst freigegebene Daten, Funktion, u. U. dienstliche Telefonnummer)
- Gruppenzugehörigkeiten in Teams
- Unterrichtsmaterial, Aufgaben

Weitere Detailangaben sind im Verfahrensverzeichnis des Verantwortlichen aufgeführt.

Beschreibung des Angebots

Microsoft Office 365 bietet mit Microsoft Teams eine Lernplattform an. Dies ist ein intuitives, geräte- und orts-unabhängiges soziales Medium unter Kontrolle der Schule, das eine Messenger-ähnliche Kommunikation mit der Bereitstellung von Texten, Dokumenten, Bildern, Videos ermöglicht. Damit verknüpft ist ein modernes E-Mailsystem und Microsoft Office in der aktuellen Form, das lokal sowohl auf allen Schulgeräten, als auch auf den privaten Geräten der Schüler und Mitarbeiter installiert werden kann.

- Die Software steht auf allen üblichen Medien wie PCs, Macs, Tablets, Handys zur Verfügung und kann von all diesen Medien ortsunabhängig genutzt werden.
- Die Software steht für Schüler, Lehrer und Mitarbeiter einer Schule kostenlos zur Verfügung und kann jeweils gleichzeitig auf bis zu 10 Geräten installiert und genutzt werden.
- In Teams integriert sind E-Mail und Kalender, es können weitere Lernprogramme vom Lehrer in Teams integriert werden. Somit erhält jeder Schüler automatisch eine E-Mailadresse, über die dieser E-Mails empfangen und senden kann.
- Das System bietet die Möglichkeit, das Versenden von E-Mails auf die Mitglieder der Schule zu beschränken. Ebenso bietet das System die Möglichkeit, den Austausch von Dokumenten oder anderen Daten auf Mitglieder der Schule zu beschränken.
- Jeder Schüler hat einen eigenen Arbeitsbereich, der nur vom jeweils zuständigen Lehrer eingesehen werden kann, aber nicht von anderen Schülern. Lehrer können Dateien, Bilder und Videos bereitstellen, Aufgaben mit Abgabeterminen erstellen und diese Aufgaben bewerten. Schüler und Lehrer können untereinander und miteinander vertraulich Nachrichten austauschen.
- Grundsätzlich können sich die Systembetreuer Einsicht in alle gespeicherten Daten verschaffen und diese redigieren oder löschen, falls dies aus pädagogischen oder rechtlichen Gründen in Absprache mit den verantwortlichen Vertretern der Schulleitung, der Lehrer, der Eltern oder der Schülervertreter geboten ist.
- Für Lehrer und Mitarbeiter der Schule bietet Office 365 eine Ende-zu-Ende-Verschlüsselung der Daten und Mehrfaktoranmeldung an, um die Sicherheit der Daten nach Stand der Technik zu gewährleisten.

Datenschutzrechtliche Aspekte

Der Einsatz einer digitalen Lernplattform schließt die automatisierte Verarbeitung personenbezogener Daten ein. Dies ist nach Artikel 6, Abs. 1 lit. c) und e) der DSGVO aufgrund unserer oben genannten Verpflichtung einer Schule rechtskonform.

Die Datenschutzverantwortung liegt bei unserer Schule. Wir legen fest, welche Daten gespeichert werden, wer darauf Zugriff hat, wer über die gespeicherten Daten Auskunft geben kann, welche Fristen für die Löschung der Daten nach Verlassen der Schule gelten.

Verfügbarkeit

Microsoft garantiert eine weltweite Verfügbarkeit der Office 365 Dienste mit 99,9 % Wahrscheinlichkeit. Alle in Office 365 (OneDrive) gespeicherten Daten können auf lokalen Geräten synchronisiert werden, sodass Sie auch ohne Internet verfügbar sind.

Sicherheit und Integrität der Daten und der Schutz vor Identitätsdiebstahl

Office 365 ermöglicht eine Ende-zu-Ende Verschlüsselung aller E-Mails und Dokumente. Das Verfahren heißt Azure Information Protection und ermöglicht dem Lehrer, Dokumente auf einfache Weise so zu schützen, dass diese nur mehr von den voreingestellten Gruppen von Benutzern von Office 365 geöffnet und gelesen oder gelesen und geändert werden können. Diese Verschlüsselung ist zertifikatsbasiert.

Office 365 bietet standardmäßig eine komfortable Mehrfaktoranmeldung an, wobei der Benutzer selbst aus einer ganzen Reihe von Anmeldefaktoren wählen kann. Diese Anmeldedaten sind auch den Administratoren nicht zugänglich und können nur vom Benutzer selbst geändert werden.

Vertraulichkeit der Daten und Nichtverketzung

Die Vertraulichkeit der in Office 365 gespeicherten Daten ist durch detaillierte Rechtezuweisungen garantiert. Standardmäßig sind vom Benutzer gespeicherte Daten nur für ihn selbst zugänglich und er muss diese explizit anderen Benutzern zum Lesen oder zum Lesen und Bearbeiten freigeben.

Schutz der Privatsphäre

Auf allen Geräten laufen Office 365 Apps wie Word, Excel, PowerPoint, SharePoint, OneNote, OneDrive oder Teams sowie Outlook am Web in einem Isolationsmodus, sodass andere Apps keinen Zugriff auf diese Daten erhalten.

Intervenierbarkeit und Widerspruch

Jedes Mitglied der Schule hat das Recht, nicht nur Auskunft, sondern auch eine rasche Korrektur der personenbezogenen Daten zu verlangen, wenn diese nicht aktuell oder richtig sind. Außerdem kann jedes Mitglied der Speicherung weiterer personenbezogener Daten, die über das oben angegebene Minimum hinausgehen, jederzeit zu widersprechen. Dies ist formlos beim Datenschutzbeauftragten des Schulamtes Nürtingen möglich.

Technische und organisatorische Maßnahmen

Die technisch-organisatorischen Maßnahmen in den EU-Rechenzentren von Microsoft Irland sind durch die Zertifizierung und die Angaben in diesem Link <http://www.trustcenter.office365.de> aufgeführt. Die verbleibenden Maßnahmen sind im Verfahrensverzeichnis des Verantwortlichen beschrieben.

Eingriff in Grundrechte

Wie dargelegt, sind die personenbezogenen Daten in Office 365 sicher nach Stand der Technik und inkludieren nur die minimalen Daten, die für die Erledigung der schulischen Aufgaben erforderlich ist.

Der Eingriff in die Grundrechte und Grundfreiheiten der Benutzer wird durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam auf ein minimales Risiko reduziert.

Zugriff auf Daten

Zugriff auf die Daten haben unsere aktuell bestimmten schulischen Systembetreuer und der von uns mit der Ersteinrichtung der Office 365 Konten beauftragte Dienstleister mit dem ein gesonderter Auftragsverarbeitungsvertrag für diesen Zweck abgeschlossen wurde.

Auskunft über gespeicherte Daten

Geben die schulischen Systembetreuer und der Datenschutzbeauftragte des Schulamtes Nürtingen.

Löschfristen

Ein Office 365 Schülerkonto (bzw. Lehrerkonto) wird inklusive aller gespeicherten Daten 4 Wochen (bzw. 3 Monate) nach Verlassen der Schule irreversibel gelöscht.

Prüfung durch Datenschutzbeauftragten

Der Datenschutzbeauftragte der Gemeinde Lenningen hat das Angebot von Office 365 geprüft und die Erfüllung der datenschutzrechtlichen Anforderungen des Angebots in der beabsichtigten Einsatzform bestätigt.

Beschlusspunkte

1. Umfang: Es besteht Einvernehmen, dass der Einsatz digitaler Medien nicht zu einer Mehrbelastung der Schüler führen darf. Eltern können sich bei dahingehenden Problemen oder Fragen an unseren Systembetreuer oder an die Schulleitung persönlich, schriftlich, per E-Mail oder per Telefon melden.
2. Lehrer: der Einsatz und Umfang des Einsatzes von Office 365 in einem Fach, einer Klasse oder Unterrichtseinheit obliegt der freien Entscheidung des jeweiligen Lehrers.
3. Schüler: Schüler können Vorschläge, Probleme oder Fragen zu dem Einsatz der Lernplattform an die Schülervertreter, an ihren Klassenlehrer oder an den Systembetreuer persönlich melden.

4. Es wird vereinbart, dass E-Mails auch mit Externen ausgetauscht werden können, das Teilen von Daten mit Externen aber eine Anmeldung an einen Microsoft Dienst oder einen per E-Mail zugestellten Code erfordert.

5. Dauer: diese Vereinbarung zum Einsatz von Office 365 als Lernplattform gilt ab Beschluss 1 Jahr und endet danach. Nach diesem Jahr evaluiert dieses Gremium diese Vereinbarung und kann danach eine Verlängerung beschließen. Die Regeln für die Gültigkeit des Beschlusses folgen aus der Satzung des Gremiums.

Anhang zum Beschluss: Genutzte Microsoft 365 Dienste

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

Azure Active Directory, Azure Information Protection, Mehrfaktorauthentifizierung

Funktion: Das Azure Active Directory (AAD) ist der zentrale Verzeichnisdienst für alle Office 365 Anwendungen. Es dient in erster Linie zur Authentifizierung der Benutzer und der Registrierung von Geräten, um Single-Sign-On zu ermöglichen.

Verarbeitete Daten: Name, Vorname, E-Mail-Adresse, 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 Office 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.

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 Name, Vorname, E-Mail-Adresse, Inhaltsdaten von E-Mail, 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 Sicherstellung 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.

Security & Compliance

Funktion Office 365 enthält eine Vielzahl von Funktionen, die dabei unterstützen sollen, die Systemsicherheit sowie die Compliance der Organisation sicherstellen zu können.

Verarbeitete Daten: Name, Vorname, E-Mail-Adresse, Weitere Profileigenschaften eines Benutzers, Metadaten zur Kommunikation und Produktnutzung

Berichte zwecks Sicherstellung 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

Teams

Funktion Microsoft Teams ist einerseits eine Messenger-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 dabei. Diese unterstützt das Lehrer-/Schüler-Verhältnis mit angepassten Zugriffsrechten, Aufgabenteilung und Aufgabenbewertung.

| | |
|----------------------|---|
| Verarbeitete Daten | Name, Vorname, E-Mail-Adresse, Weitere Profileigenschaften eines Benutzers, Präsenzinformationen, Metadaten zur Kommunikation und Produktnutzung, Inhalte der Klassennotizbücher. |
| Löschfristen | Teams mit Klassennotizbüchern der Lehrer und Schüler 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 |

OneDrive

| | |
|--------------------|--|
| Funktion | Auf OneDrive können Sie Ihre persönlichen Dateien an einem zentralen Ort speichern, für andere Personen freigeben und von jedem mit dem Internet verbundenen Gerät aus darauf zugreifen. |
| Verarbeitete Daten | Name, Vorname, E-Mail-Adresse, Inhaltsdaten, Metadaten zur Kommunikation und Produktnutzung |

Sharepoint

| | |
|--------------------|---|
| Funktion | Organisationen verwenden Microsoft SharePoint zum Erstellen von Websites. Sie können SharePoint als sicheren Ort zum Speichern, Strukturieren und Freigeben von sowie zum Zugreifen auf Informationen von nahezu allen Geräten aus verwenden. |
| Verarbeitete Daten | Name, Vorname, E-Mail-Adresse, Inhaltsdaten, Metadaten zur Kommunikation und Produktnutzung |

Office

| | |
|--------------------|---|
| Funktion | Die Webanwendungen beinhalten Online-Versionen von Anwendungen wie Word, Excel, PowerPoint, OneNote, Outlook und werden oft auch unter dem Namen Microsoft Office Online zusammengefasst. Microsoft Office Online stellt eine eigenständige Lösung dar, die die Office-Anwendungen von jedem Rechner mit Browser und Online-Verbindung unabhängig vom installierten Betriebssystem nutzbar macht. |
| Verarbeitete Daten | Name, Vorname, E-Mail-Adresse, Inhaltsdaten, Metadaten zur Kommunikation und Produktnutzung |

Anhang 2

Nutzungsordnung für das pädagogisches Netz der Karl-Erhard-Scheufelen Schulen

Vorabbemerkung

Die Nutzungsordnung als Ergänzung zur gültigen Hausordnung der Schule gilt für die Benutzung der schulischen IT-Systeme und Computer (inklusive Tablets) an der Schule innerhalb und außerhalb des Unterrichts. Sie trägt dazu bei, ein höheres Maß an Datenschutz und einen optimalen Zustand dieser Einrichtungen zu gewährleisten. Dies ist Voraussetzung dafür, dass jederzeit effektiv mit den neuen Medien gearbeitet werden kann.

Liebe Schülerinnen und Schüler, liebe Eltern

Für die Arbeit an der Schule steht allen Schülerinnen und Schülern ein Zugang zum Internet, ein Microsoft Office 365 Konto mit verschiedenen Online-Diensten und Office ProPlus zur Nutzung für alle Arbeiten im Rahmen des Unterrichts zu Hause und in der Schule zur Verfügung. Alle Schülerinnen und Schüler werden gebeten, zu einem reibungslosen Betrieb beizutragen und die notwendigen Regeln einzuhalten.

Der besseren Verständlichkeit halber wird im Weiteren die grammatikalisch männliche Form verwendet, sie gilt aber in gleicher Weise unabhängig vom Geschlecht.

Allgemeine Rahmenbedingungen

1. Datenschutz und Datensicherheit

Bitte beachten Sie, dass sich die Schule grundsätzlich über den Administrator Zugriff zu allen in Office 365 gespeicherten Daten verschaffen kann. Sie wird dies nur tun, wenn dies begründet ist, zum Beispiel ein Verdacht auf Missbrauch oder unangemessener Nutzung besteht oder dies für die Gewährleistung der technischen Sicherheit und Unversehrtheit der Daten notwendig erscheint. In jedem Fall werden die betroffenen Schülerinnen und Schüler und ggf. die Erziehungsberechtigten darüber informiert.

2. Passwörter

- Wir richten für alle Schüler Office365-Konten mit einem Passwort ein, das Sie selbst ändern können.
- Bitte halten Sie das persönliche Passwort geheim. Sie könnten für missbräuchliche Verwendung Ihres Kontos zur Verantwortung gezogen werden.
- Es ist nicht statthaft, sich als ein anderer Schüler oder gar als Lehrer anzumelden.
- Vergessen Sie bitte nie, sich nach Beendigung der Nutzung von Ihrem Konto abzumelden. Dies dient Ihrer eigenen Sicherheit.

Wir weisen darauf hin, dass bei der Erstellung eines eigenen Kennwortes folgende Maßgaben zu beachten sind: Mindestlänge 8 Zeichen bestehend aus Buchstaben, Zahlen, Groß- und Kleinschreibung und Sonderzeichen (z.B.: # ! & ?).

3. Bereitstellung und Nutzung von digitalen Materialien

- Wenn Sie Daten in Office 365 ablegen und anderen Personen freigeben, achten Sie bitte darauf, dass Sie dazu berechtigt sind. Es könnte sein, dass der Urheber der Daten eine Weitergabe nicht gestattet. Sie sind dafür verantwortlich, die Bestimmungen des Urheberrechts einzuhalten.
- Wenn Sie Daten aus dem Internet im Zusammenhang mit dem Unterricht einsetzen, achten Sie bitte darauf, die Quelle der Information oder der Daten sorgfältig anzugeben.
- Sollten Sie Kenntnis erlangen, dass rechtswidrige Inhalte wie gestohlene Musik oder Filme oder Inhalte, die Gewalt, Hass und Hetze verbreiten, gespeichert oder geteilt werden, informieren Sie bitte sofort eine Lehrkraft Ihres Vertrauens oder den Datenschutzbeauftragten des Schulamtes.

4. Nutzung von Informationen aus dem Internet

- Der Internet-Zugang soll grundsätzlich nur für Zwecke genutzt werden, die einem schulischen Zweck dienen. Hierzu zählt auch ein elektronischer Informationsaustausch, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit dem Unterricht an der Schule im Zusammenhang steht.
- Die Nutzung von weiteren Anwendungen (z.B. durch Herunterladen aus dem Internet) muss im Zusammenhang des Unterrichts stehen.
- Im Namen der Schule dürfen weder Vertragsverhältnisse eingegangen noch kostenpflichtige Dienste im Internet benutzt werden.
- Die Schulleitung ist nicht für den Inhalt der über Ihren Internet-Zugang abrufbaren Angebote verantwortlich.

5. Verbotene Nutzungen

Es ist verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen.

6. Eingriffe in die Hard- und Softwareinstallation

- Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzwerkes sowie Manipulationen an der Hardwareausstattung sind grundsätzlich untersagt.
- Bitte vermeiden Sie unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien (zum Beispiel Grafiken, Videos, etc.)

7. Schutz der Geräte

- Die Bedienung der Hard- und Software hat entsprechend der Instruktionen zu erfolgen. Störungen oder Schäden sind sofort der für die Computernutzung verantwortlichen Person oder dem Systembetreuer zu melden. Wer schuldhaft Schäden verursacht, muss für deren Behebung aufkommen.
- Die Tastaturen sind durch Schmutz und Flüssigkeiten besonders gefährdet, deshalb ist in den Computerräumen Essen und Trinken grundsätzlich verboten.

8. WLAN-Zugang

- Die Authentifizierung erfolgt bei schuleigenen Geräten (Notebooks, Tablets, etc.) über einen WPA2 Zugang. Die Zugangsdaten wurden in den schuleigenen Geräten gespeichert.
- Die Nutzung des WLANs erfolgt in der Regel nur zu schulischen Zwecken.

Lernplattform Office 365 Education

An unserer Schule wird Office365 Education als Lern – und Kommunikationsplattform eingeführt. Diese Plattform ist für die Nutzer kostenlos und ermöglicht eine unserem Medienkonzept entsprechend moderne und zukunftsweisende Zusammenarbeit zwischen den Lehrenden und Lernenden.

Dem Benutzer wird dabei während seiner Schulzeit ein Benutzerkonto auf der Online-Plattform Office 365 Education zur Verfügung gestellt. Der Zugriff auf diese Dienste erfolgt über die Seite <https://portal.office.com> oder alternativ über die Seite <https://teams.microsoft.com>. Diese Dienste enthalten:

- Eine E-Mail-Adresse und ein bis zu 50 GB großes Postfach;
- die Bereitstellung des Cloudspeichers OneDrive der Schule mit bis zu 1 TB Datenspeicher;
- die chat-basierte Lernplattform Teams, die jedem Schüler für jedes Fach ein eigenes OneNote Notizbuch zur Verfügung stellt, und die Ablage von Daten und Dokumenten ermöglicht.

Nutzung von Chat und Anlage von Teams

- Bitte achten Sie darauf, nur Personen per Chat zu kontaktieren, die dazu Ihre Einwilligung gegeben haben. Wenn sich eine Schülerin oder ein Schüler nicht daranhält, kann ihr oder ihm die Chat-Funktion für eine bestimmte Zeit entzogen werden.

- Wenn Schüler eigene Teams anlegen dürfen, muss der Team-Name einen klar erkennbaren Schulbezug haben.

Verbotene Aktionen in Teams-Besprechungen

- Es ist verboten, Personen gegen ihren Willen anzuschatten.
- Es ist verboten, andere Teilnehmer einer Teams-Besprechung durch mutwillige Aktionen zu stören.
- Es ist verboten, Teams-Sitzungen ohne Zustimmung aller Teilnehmer aufzuzeichnen.
- Es ist Schülern verboten, schulexternen Personen die Teilnahme an einer Teams-Besprechung zu genehmigen.

Die Schule behält sich vor, einzelne Dienste nicht zur Verfügung zu stellen. Beim Verlassen der Schule wird das Benutzerkonto deaktiviert und gelöscht. Alle vorhandenen Daten werden zu diesem Zeitpunkt ebenfalls gelöscht.

Die Einführung von Office 365 in unserer Schule ist datenschutzrechtlich geprüft und wurde von der Schulleitung, den Vertretern der Lehrer, der Eltern und der Schüler zum 14.07.2025 genehmigt. Die von Schülern oder Lehrern in Office 365 abgelegten Daten werden ausschließlich innerhalb der EU gespeichert, sie werden weder durchsucht noch an Dritte weitergegeben.

Schlussvorschriften

Die Schülerinnen und Schüler werden zu Beginn der schulischen Nutzung über diese Nutzungsordnung unterrichtet. Sie versichern durch ihre Unterschrift, dass sie diese anerkennen. Diese Belehrung wird im Schultagebuch protokolliert und jedes Jahr, zu Beginn des Schuljahres, wiederholt. Diese Benutzerordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt am Tage nach ihrer Bekanntgabe an der Schule in Kraft.

Zu widerhandlungen gegen diese Nutzungsordnung können den Entzug der Nutzungsberechtigung und ggf. rechtliche Konsequenzen und die unverzügliche Pflicht zur Rückgabe der überlassenen Soft- und Hardware zur Folge haben.

Anhang 3

Datenschutzerklärung zur Nutzung von Microsoft Office 365

Verantwortlicher

gem. Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (EU-DSGVO)
Karl-Erhard-Scheufelen Schule
Theresa-Maria Breier
Tobelstraße 5
73252 Lenningen

poststelle@dienststellenummer.schule.bwl.de

Datenschutzbeauftragter

Staatliches Schulamt Nürtingen
Datenschutzbeauftragter
Marktstraße 12
72622 Nürtingen

datenschutz@ssa-nt.kv.bwl.de

Zweck der Datenverarbeitung

- IT-gestützte Zusammenarbeit der Mitarbeiter und Schüler der Schule mittels der Microsoft Office 365 Dienste Exchange Online, Sharepoint Online und der Lernplattform Teams.
- Unterstützung von Schulen bei der Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben mit Hilfe von Microsoft Office365 zur Umsetzung des Bildungs- und Erziehungsauftrags, bei der Abwicklung der schulinternen Aufgaben und Abläufe und der Umsetzung der Medienkompetenzen im Rahmen der Digitalisierung.

Besonders sind dies:

- E-Mailkommunikation mit Termin- und Ressourcenverwaltung, gemeinsame Kalender, Office 365 Gruppen
- Bereitstellung und Austausch von Dokumenten
- Projektverwaltung zur Organisation der schulischen Abläufe, Chatfunktion
- Lernplattform Teams mit Klassennotizbüchern, Bereitstellung von Unterrichtsmaterialien, Aufgaben mit Terminabgabe, Bewertung, Rückmeldung
- Nutzung der Desktopversion von Office

Rechtsgrundlage

- Bestimmungen der Schulordnungen, des Schulgesetzes und der Lehrerdienstordnung
- Art. 6 Abs. 1 S. 1 lit. c) und e) DSGVO i.V.m. § 1 und § 38 Abs.6 SchG BW

Kategorien betroffener Personen

- Lehrkräfte, nicht unterrichtendes Personal, Verwaltungspersonal der Schule sowie externes Betreuungspersonal, das an der Schule tätig ist
- Alle Schüler, die im laufenden Schuljahr die Schule besuchen oder besucht haben

Kategorien der Daten, die verarbeitet werden

Daten zu Lehrkräften und zum nicht unterrichtenden Personal

- Grunddaten (Name, Vornamen, Anzeigenname, Anmeldenname, E-Mailadresse, weitere dienstliche E-Mailadressen, Funktion, dienstliche Telefonnummer falls bestehend)
- Gruppenzugehörigkeiten in Teams, Mitbesitzer eines Teams, unterrichtete Fächer, unterrichtete Klassen

Daten der Schüler

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion)
- Schulart, Klasse, Jahrgangsstufe
- Besuchte Unterrichtseinheiten, für die Teams eingerichtet werden
- Unterrichtselemente (Lehrstoff, Leistungserhebungen, Aufgabenzuteilungen, Bewertungen)

Daten aller Nutzer

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion)
- Berechtigungen
- Log-Daten (Datum der letzten Passwortänderung, Datum der letzten Anmeldung, Größe und Zahl der gespeicherten Daten)
- Historisierung (Information über angelegte/geänderte/gelöschte Datensätze)

Von den Nutzern erzeugte Inhalte und Einstellungen

- persönliche Einstellungen, Angaben in Nutzerprofil, gespeicherte Inhalte in E-Mail, Chats, Kalendereinträge, Kommentare, Datenbankeinträge, Daten der unterrichteten bzw. verwalteten Schüler
- Weitere Faktoren zur Anmeldung mittels Multi-Faktor-Authentifizierung (Telefon oder private E-Mail oder App oder Fragen)

Es werden keine Daten der besonderen Kategorien nach Art. 9 DSGVO verarbeitet.

Geplante Speicherdauer

Verlässt ein Mitarbeiter die Schule, wird sein persönliches Office 365 Konto inklusive aller gespeicherten Daten nach 3 Monaten gelöscht. Die Rechte auf weitere Office 365 Konten werden ihm gleichzeitig entzogen.

Empfänger oder Kategorie von Empfängern der Daten

| | Empfänger | Zweck | Daten |
|--------|---|--|---|
| Intern | Mitarbeiter & Schüler | Zusammenarbeit und IT-gestützter Unterricht | Eingeschränkte Lese- und/oder Schreibrechte in den Teams und Office 365 Gruppen, deren Mitglied sie sind und in den Dokumentenbibliotheken und öffentlichen Kalendern, die ihnen freigegeben wurden |
| | Systembetreuer | Konfiguration, Überwachung und Sicherung des Betriebs, Support | Administrative Lese-, Schreib- und Löschrechte entsprechend den ihnen zugeteilten Rechten auf alle oder bestimmte Office 365 Dienste |
| Extern | Alle Empfänger von E-Mails | Kommunikation | Anzeigename, E-Mail-Adresse |
| | Ireland Operations Limited, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Irland | Dienstbereitstellung, Service und Support | <ul style="list-style-type: none">• von den Benutzern gespeicherte Daten: Die Speicherung erfolgt nur innerhalb der EU in nach ISO 27001, 27002, ISO/IEC 27018 zertifizierten Rechenzentren im Rahmen des AV-Vertrags http://aka.ms/Wkcowi, der die EU Standardvertragsklauseln enthält. |

| | | | |
|--|--|--|--|
| | | | <ul style="list-style-type: none"> • Anmeldezeiten: Speicherung in allen Microsoft-Anmeldeservern |
|--|--|--|--|

Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)

- Microsoft Ireland beschäftigt Unterauftragsnehmer in Drittländern, insbesondere Microsoft Corporation in USA, die sich den EU-Standardvertragsklauseln unterworfen haben. Diese Unterauftragsnehmer sind unter folgendem Link vollständig aufgeführt: <https://www.microsoft.com/de-de/trustcenter/privacy/data-management/data-access>.
- Wenn ein neuer Dienst in Office 365 angeboten wird, werden die damit verbundenen Daten in USA verarbeitet. Diese Dienste werden vom Systembetreuer ausgeschaltet.

Technische und Organisatorische Maßnahmen

Die Schule stellt die Einhaltung von technischen und organisatorischen Maßnahmen nach Maßgabe der DSGVO und nach Stand der Technik sicher, um Personendaten von Schülern und Lehrkräften zu gewährleisten. Detailinformationen können auf Nachfrage eingesehen werden.

Betroffenenrechte

Sie haben als von einer Verarbeitung personenbezogener Daten betroffene Person folgende Rechte:

- Gemäß Artikel 15 EU-DSGVO können Sie Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten verlangen. Insbesondere können Sie Auskunft über die Verarbeitungszwecke, die Kategorie der personenbezogenen Daten, die Kategorien von Empfängern, gegenüber denen Ihre Daten offengelegt wurden oder werden, die geplante Speicherdauer, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts, die Herkunft ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten verlangen.
- Gemäß Artikel 16 EU-DSGVO können Sie die unverzügliche Berichtigung unrichtiger oder Vervollständigung Ihrer bei uns gespeicherten personenbezogenen Daten verlangen.
- Gemäß Artikel 17 EU-DSGVO können Sie die Löschung Ihrer bei uns gespeicherten personenbezogenen Daten verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.
- Gemäß Artikel 18 EU-DSGVO können Sie die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten verlangen, soweit die Richtigkeit der Daten von Ihnen bestritten wird oder die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen oder wir die Daten nicht mehr benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen.
- Gemäß Artikel 21 EU-DSGVO können Sie Widerspruch gegen die Verarbeitung einlegen. Dieses Widerspruchsrecht ist das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die für die Wahrnehmung einer uns übertragenen Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Wir verarbeiten die personenbezogenen Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten Ihrer Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Gemäß Artikel 20 EU-DSGVO können Sie Ihre personenbezogenen Daten, die Sie uns per Einwilligung bereitgestellt haben und die wir automatisiert verarbeiten, in einem strukturierten, gängigen und maschinenlesebaren Format erhalten oder die Übermittlung an einen anderen Verantwortlichen verlangen (Recht auf Datenübertragbarkeit).

- Gemäß Artikel 77 EU-DSGVO können Sie sich bei einer Datenschutz-Aufsichtsbehörde beschweren. In der Regel können Sie sich hierfür an die Aufsichtsbehörde Ihres üblichen Aufenthaltsortes oder Arbeitsplatzes wenden. In Baden-Württemberg ist dies der Landesbeauftragte für den Datenschutz und die Informationsfreiheit.

Anhang 4

Technische und Organisatorische Maßnahmen (TOMs) für die Verwendung von Microsoft Office 365

Die technisch-organisatorischen Maßnahmen in den EU-Rechenzentren von Microsoft Irland sind durch die Zertifizierung und die Angaben in diesem Link <http://www.trustcenter.office365.de> aufgeführt.

Die verbleibenden Maßnahmen, die hier beschrieben wird, sind die Maßnahmen zur Sicherung des Internet-Zugangs zu den Microsoft Diensten in Office 365 und zur sicheren Speicherung von Zugangsdaten auf den Clients des Verantwortlichen.

Vertraulichkeit

(Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle: Die Anmeldung an Office 365 erfolgt im Browser per verschlüsseltem und eingeschränktem Authentifizierungsverfahren nach dem OAuth2 Protokoll. Die Büroräume sind nur berechtigten Personen zugänglich und außerhalb der Dienstzeiten versperrt.
- Zugangskontrolle: E-Mail in Office 365 ist durch die Sichere-Links- und Sichere-Anhangs-Technologie geschützt. Die Desktop Betriebssysteme der Verwaltungsmitarbeiter und Systembetreuer sind Windows 10 Professional und durch Applikations- und Makro-Kontrolle geschützt.
- Zugriffskontrolle: Die Geräte und Konten sind durch Benutzername und Passwort gesichert. Alle Lehrkräfte als Nutzer eines mobilen Endgeräts haben eine bestimmte datenschutzrechtliche Nutzungsbedingungen unterzeichnet.
- Trennungskontrolle: Administrativer Zugriff auf die Office 365 Instanz der Schule ist auf die vom Schulleiter bestellten Systembetreuer beschränkt.

Integrität

(Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle: Im Rahmen der Nutzung von Microsoft Online Diensten liegt die Umsetzung der Weitergabekontrolle bei Microsoft. Microsoft setzt im Rahmen der Online Dienste bei der Datenübertragung über das Internet auf TLS-Verschlüsselung (https Protokoll).
- Eingabekontrolle: Die Konsistenz und Gültigkeit der Benutzerkonten in den Office 365 Instanzen ist durch die tägliche Anmeldung der Benutzer, die Sichtbarkeit der Benutzerkonten in den Adresslisten und Verzeichnissen gewährleistet.

Verfügbarkeit und Belastbarkeit

(Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle: Alle Benutzer-Anmeldedaten und Nutzerdaten liegen in den Microsoft EU Rechenzentren (die für deutsche Kunden in Frankfurt und Berlin liegen) und sind durch die spezifischen Sicherheitsmaßnahmen von Microsoft geschützt, insbesondere durch die Backup-Strategien von Microsoft (Datei-Versionierung, Spiegelung der virtuellen Instanzen).
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO): Dies ist serverseitig durch die mehrfache Spiegelung der virtuellen Instanzen in den Office 365 Instanzen gesichert (Microsoft Servicevertrag), Nutzerdaten in Office 365 können vom Nutzer selbst mit einem Klick auf den Stand eines früheren Zeitpunkts wiederhergestellt werden.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management: Die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird durch die Zertifizierung des Auftragnehmers gemäß Art. 42 DSGVO gesichert.
- Incident-Response-Management: Falls ein illegitimer Zugriff auf eine Office 365 Instanz erfolgt, sind 2 Szenarien möglich: es werden zusätzliche Konten erstellt oder es werden Konten gelöscht. Gelöschte Konten und damit zusammenhängende Daten und E-Mails können in Office 365 teils durch den Nutzer selbst, und teils durch einen speziellen Papierkorb, auf den nur der Administrator

Zugriff hat, wiederhergestellt werden. Zusätzliche Konten erscheinen in den Adressbüchern und können kurzfristig gelöscht werden.

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO):** Die Mitarbeiter werden von den Systembetreuern auf die Möglichkeiten der Pseudonymisierung und sparsamen Speicherung personenbezogener Daten in Office 365 hingewiesen und dabei unterstützt.
- **Auftragskontrolle:** Die Office 365 Instanz gehört dem Auftraggeber, der alleine Zugriff auf die Nutzdaten hat.

Anhang 5

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gem. Artikel 30 Abs. 1 DSGVO

Name des eingesetzten Verfahrens & Dienstbeschreibung

Office365 – Exchange Online, SharePoint Online, Teams, Installation der Desktopanwendungen

Microsoft Office 365 (<http://aka.ms/Wkcowi>)

<https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx> und
<https://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx>

Zweck der Datenverarbeitung

- IT-gestützte Zusammenarbeit der Mitarbeiter und Schüler der Schule mittels der Microsoft Office 365 Dienste Exchange Online, Sharepoint Online und der Lernplattform Teams.
- Unterstützung von Schulen bei der Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben mit Hilfe von Microsoft Office365 zur Umsetzung des Bildungs- und Erziehungsauftrags, bei der Abwicklung der schulinternen Aufgaben und Abläufe und der Umsetzung der Medienkompetenzen im Rahmen der Digitalisierung.

Besonders sind dies:

- E-Mailkommunikation mit Termin- und Ressourcenverwaltung, gemeinsame Kalender, Office 365 Gruppen
- Bereitstellung und Austausch von Dokumenten
- Projektverwaltung zur Organisation der schulischen Abläufe, Chatfunktion
- Lernplattform Teams mit Klassennotizbüchern, Bereitstellung von Unterrichtsmaterialien, Aufgaben mit Terminabgabe, Bewertung, Rückmeldung
- Nutzung der Desktopversion von Office

Rechtsgrundlage

- Bestimmungen der Schulordnungen, des Schulgesetzes und der Lehrerdienstordnung
- Art. 6 Abs. 1 S. 1 lit. c) und e) DSGVO i.V.m. § 1 und § 38 Abs.6 SchG BW

Kategorien betroffener Personen

- Lehrkräfte, nicht unterrichtendes Personal, Verwaltungspersonal der Schule sowie externes Betreuungspersonal, das an der Schule tätig ist
- Alle Schüler, die im laufenden Schuljahr die Schule besuchen oder besucht haben

Kategorien der Daten, die verarbeitet werden

Daten zu Lehrkräften und zum nicht unterrichtenden Personal

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, E-Mailadresse, weitere dienstliche E-Mailadressen, Funktion, dienstliche Telefonnummer falls bestehend)
- Gruppenzugehörigkeiten in Teams, Mitbesitzer eines Teams, unterrichtete Fächer, unterrichtete Klassen

Daten der Schüler

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion)
- Schulart, Klasse, Jahrgangsstufe
- Besuchte Unterrichtseinheiten, für die Teams eingerichtet werden
- Unterrichtselemente (Lehrstoff, Leistungserhebungen, Aufgabenzuteilungen, Bewertungen)

Daten aller Nutzer

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion)
- Berechtigungen
- Log-Daten (Datum der letzten Passwortänderung, Datum der letzten Anmeldung, Größe und Zahl der gespeicherten Daten)
- Historisierung (Information über angelegte/geänderte/gelöschte Datensätze)

Von den Nutzern erzeugte Inhalte und Einstellungen

- persönliche Einstellungen, Angaben in Nutzerprofil, gespeicherte Inhalte in E-Mail, Chats, Kalendereinträge, Kommentare, Datenbankeinträge, Daten der unterrichteten bzw. verwalteten Schüler
- Weitere Faktoren zur Anmeldung mittels Multi-Faktor-Authentifizierung (Telefon oder private E-Mail oder App oder Fragen)

Es werden keine Daten der besonderen Kategorien nach Art. 9 DSGVO verarbeitet.

Geplante Speicherdauer

Verlässt ein Mitarbeiter die Schule, wird sein persönliches Office 365 Konto inklusive aller gespeicherten Daten nach 3 Monaten gelöscht. Die Rechte auf weitere Office 365 Konten werden ihm gleichzeitig entzogen.

Empfänger oder Kategorie von Empfängern der Daten

| | Empfänger | Zweck | Daten |
|---------------|--|--|---|
| Intern | Mitarbeiter & Schüler | Zusammenarbeit und IT-gestützter Unterricht | Eingeschränkte Lese- und/oder Schreibrechte in den Teams und Office 365 Gruppen, deren Mitglied sie sind und in den Dokumentenbibliotheken und öffentlichen Kalendern, die ihnen freigegeben wurden |
| | Systembetreuer | Konfiguration, Überwachung und Sicherung des Betriebs, Support | Administrative Lese-, Schreib- und Löschrechte entsprechend den ihnen zugeteilten Rechten auf alle oder bestimmte Office 365 Dienste |
| Extern | Alle Empfänger von E-Mails | Kommunikation | Anzeigename, E-Mail-Adresse |
| | Ireland Operations Limited, Carmanhall Road, Sandymount Industrial Estate, Dublin 18, Irland | Dienstbereitstellung, Service und Support | <ul style="list-style-type: none">• von den Benutzern gespeicherte Daten: Die Speicherung erfolgt nur innerhalb der EU in nach ISO 27001, 27002, ISO/IEC 27018 zertifizierten Rechenzentren im Rahmen des AV-Vertrags http://aka.ms/Wkcowi, der die EU Standardvertragsklauseln enthält.• Anmeldedaten: Speicherung in allen Microsoft-Anmeldeservern |

Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)

- Microsoft Ireland beschäftigt Unterauftragsnehmer in Drittländern, insbesondere Microsoft Corporation in USA, die sich den EU-Standardvertragsklauseln unterworfen haben. Diese

Unterauftragnehmer sind unter folgendem Link vollständig aufgeführt:

<https://www.microsoft.com/de-de/trustcenter/privacy/data-management/data-access>.

- Wenn ein neuer Dienst in Office 365 angeboten wird, werden die damit verbundenen Daten in USA verarbeitet. Diese Dienste werden vom Systembetreuer ausgeschaltet.

Technische und Organisatorische Maßnahmen

Siehe Anhang 4