Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München
Telefon: +49 (0)89/3176-0
Telefax: +49 (0)89/3176-1000
www.microsoft.com/germany

Microsoft Deutschland GmbH · Walter-Gropius-Straße 5 · 80807 München

Herrn OStD Kai A. Richter
Friedrich-Dessauer-Gymnasium
Schulzentrum / Stadtbadstraße 4
63741 Aschaffenburg

München, den 30. April 2020

Hinweise zum Datenschutz beim Einsatz von Microsoft Office 365 in Schulen

Sehr geehrter Herr Richter,

es kursieren gegenwärtig einige Stellungnahmen zur datenschutzkonformen Nutzung von Microsoft Office 365 in Schulen oder auch darüber hinaus, die zu einem kritischen Ergebnis kommen, dabei aber von falschen oder nicht aktuellen technischen und vertraglichen Grundlagen ausgehen.

Die wesentlichsten dieser Fehleinschätzungen möchten wir hier gern korrigieren:

1. Bei der Nutzung von Microsoft Office 365 handelt es sich um Cloud-basierte Produktivitäts- und Kollaborationslösungen, die in unterschiedlichen Abonnement-Varianten angeboten werden. Hierzu gehört auch die ausschließlich online zu nutzende, kostenlose Variante Office 365 A1 für den schulischen Bereich. Die Varianten A3 und A5 erlauben die Installation von bekannten Office-Anwendungen wie Word, Excel oder PowerPoint auf einem lokalen Computer (Windows oder macOS), die dann auch offline genutzt werden können. Außerdem unterscheiden sich die Varianten im Funktionsumfang. Entsprechende Varianten existieren auch für den Unternehmensbereich.

2. Für die Nutzung all dieser Varianten im Vertragskundenbereich gelten die **Bestimmungen für Onlinedienste („OST"** – abrufbar hier**)** in Verbindung mit dem Anhang zu den **Datenschutzbestimmungen für Microsoft-Onlinedienste („OST-DPA"** – abrufbar hier**)**.
   Die Datenschutzbestimmungen (OST-DPA) für die im schulischen Bereich eingesetzten Office 365-Abonnements (A1–A5) besagen im Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse":

   „Microsoft wird Kundendaten und personenbezogene Daten nur verwenden und anderweitig verarbeiten, (a) um dem Kunden die Onlinedienste gemäß den dokumentierten Anweisungen des Kunden bereitzustellen, (b) um legitime Geschäftstätigkeiten von Microsoft zu verfolgen, die im Folgenden detailliert aufgeführt und eingegrenzt werden. ***Unter den Parteien behält der Kunde alle Rechte und das Eigentum an den Kundendaten.*** *Mit Ausnahme der Rechte, die der Kunde Microsoft in diesem Abschnitt gewährt, erwirbt Microsoft keine weiteren Rechte an Kundendaten. […]"*

Bei den unter (b) erwähnten ***„legitimen Geschäftstätigkeiten von Microsoft"*** heißt es ausdrücklich:

„Bei der Verarbeitung für legitime Geschäftstätigkeiten von Microsoft wird Microsoft Kundendaten oder personenbezogene Daten ***nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (a) Benutzerprofilierung oder (b) Werbung oder ähnliche kommerzielle Zwecke.*** Wenn Microsoft diese Daten für legitime Geschäftstätigkeiten verarbeitet, erfolgt diese Verarbeitung ausschließlich zu den in diesem Abschnitt genannten Zwecken."

Es findet damit ausdrücklich weder eine ***„Verhaltensanalyse"*** noch jedwede Art der ***„Monetarisierung von personenbezogenen Daten"*** durch Microsoft statt (zum Beispiel auch keine Nutzung zu Werbezwecken).

Die allgemeine Datenschutzerklärung von Microsoft finden Sie unter:
https://privacy.microsoft.com/de-de/privacystatement

3. Es liegt in der Natur der Sache, dass bei der Nutzung von Cloud-Diensten eine Datenübermittlung an den Anbieter der Cloud-Dienste erfolgt. Die Administration der Office 365-Anwendungen (einschließlich der Nutzerverwaltung) findet ausschließlich durch den kundenseitigen Administrator des jeweils gewählten Office 365-Pakets statt; alle Kundendaten liegen innerhalb des sogenannten Office 365-Mandanten. Microsoft-Mitarbeiter haben darauf keine dauerhaften Zugriffsrechte, sondern allenfalls in bestimmten Fällen – zum Beispiel bei Supportanfragen des Kunden mit Zustimmung des Kundenadministrators – Zugriff. Die Übermittlung der Daten von und aus der Cloud (Data in Transit) sowie die Speicherung der Daten in der Cloud (Data at Rest) sind selbstverständlich durch Verschlüsselung auf dem Stand der Technik zum Schutz der Kundendaten gewährleistet.

4. Für den Umgang mit personenbezogenen Daten im Rahmen der Auftragsverarbeitung sind alle Microsoft-Rechenzentren nach dem Standard ISO/IEC 27018:2014 zertifiziert und werden regelmäßig auditiert. Die entsprechenden Compliance- und Audit-Berichte, beispielsweise auch zum Cloud Computing Compliance Criteria Catalogue (C5)-Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI), sind öffentlich im Microsoft Trust Center verfügbar unter:
https://www.microsoft.com/de-de/trust-center/

5. Artikel 28 der DSGVO verpflichtet Auftragsverarbeiter zu Folgendem:

   - Weitere Auftragsverarbeiter nur mit Zustimmung des Verantwortlichen zu beauftragen und für diese weiteren Auftragsverarbeiter zu haften
   - Personenbezogene Daten nur auf Anweisung des Verantwortlichen zu verarbeiten, auch im Hinblick auf deren Übermittlung
   - Sicherzustellen, dass sich Personen, die personenbezogene Daten verarbeiten, der Geheimhaltung verpflichtet haben

- Geeignete technische und organisatorische Maßnahmen zu implementieren, um einen angemessenen Schutz personenbezogener Daten zu gewährleisten
- Verantwortliche bei ihrer Verpflichtung zu unterstützen, dem Auskunftsrecht betroffener Personen gemäß DSGVO nachzukommen
- Anforderungen zur Meldung von Datenschutzverletzungen und deren Klärung zu erfüllen
- Verantwortliche bei Datenschutz-Folgenabschätzungen und der Konsultation der Aufsichtsbehörden zu unterstützen
- Personenbezogene Daten nach der Erbringung der Dienstleistungen zu löschen oder zurückzugeben
- Verantwortliche durch Nachweise zur Einhaltung der DSGVO zu unterstützen

Microsoft setzt diese Anforderungen der DSGVO an eine Auftragsverarbeitungsvereinbarung im oben genannten OST-DPA vollumfänglich um.

6. In Office Online (Office 365 A1/E1) ist für die Benutzerverwaltung durch den Kundenadministrator für jeden anzulegenden Nutzer (beispielsweise SchülerIn) lediglich die Angabe eines individuellen Benutzernamens erforderlich. Für eine einfache und möglichst natürliche Zusammenarbeit zwischen LehrerIn und SchülerInnen und der SchülerInnen untereinander empfehlen wir dafür die Verwendung der Realnamen, zumal aus formalen Datenschutzgründen nichts dagegenspricht (siehe 4./5.). Gleichwohl ist es möglich, sich für die Benutzerverwaltung je Teilnehmer auf die Verwendung von Pseudonymen zu verständigen, also beispielsweise eine Zahlenkombination oder so etwas wie spitzmaus@..., zahnfee@... oder faultier@..., womit durch die Benutzerverwaltung gegenüber Office 365 kein direkter Personenbezug erforderlich ist.

7. Neben den vom Kunden erzeugten und verwalteten Daten wird häufig von „Diagnosedaten" gesprochen.

   Bei Diagnosedaten handelt es sich um technische Daten, die von Windows-Betriebssystemen, Office-Anwendungen und anderen Microsoft-Anwendungen an Microsoft gesendet werden, wenn diese von Benutzern der Kunden verwendet werden. Microsoft-Produkte und -Dienste verwenden Diagnosedaten, um Produkte und Dienste vor auftretenden Bedrohungen zu schützen (beispielweise Schadsoftware), auf aktuellem Stand zu halten und einen ordnungsgemäßen Betrieb zu gewährleisten. Kunden von Microsoft erwarten von Microsoft-Software ein hohes Maß an Stabilität, Sicherheit und Effektivität. Eine Liste der Beispiele finden Sie in dem Artikel „Diagnosedaten in Office".

   Bei **Office Online**, also auch der Varianten Office 365 A1 für Schulen oder Office 365 E1 für Unternehmen, ***werden keine Diagnosedaten vom Benutzer an Microsoft übertragen***, da die Verarbeitung direkt im Onlinedienst erfolgt und auf diesen nur über einen Browser zugegriffen wird.

   Bei den lokal installierbaren Office 365-Varianten A3/A5 beziehungsweise E3/E5 stehen dem jeweiligen Kundenadministrator umfangreiche Werkzeuge zur Verfügung, sowohl um den Umfang der Übermittlung der Diagnosedaten einzustellen als auch um hierzu Vorgaben für seine Organisation – also zum Beispiel seine Schule – zu machen und die Anwendung dieser Vorgaben

innerhalb seiner Organisation verbindlich und unumgehbar durchzusetzen. Hierbei hat der Administrator auch die Möglichkeit, die Übermittlung von Diagnosedaten komplett abzuschalten.

Mit dem Diagnostic Data Viewer steht dem Kunden (beziehungsweise dessen Administrator) zudem eine App zur Verfügung, mit deren Hilfe er sich sämtliche übermittelten Diagnosedaten ansehen kann – wodurch die Übermittlung aller Diagnosedaten transparent und analysierbar wird.

Auch für die Diagnosedaten gelten die Aussagen der unter 2. aufgeführten Datenschutzbestimmungen uneingeschränkt:
Eine ***„Verhaltensanalyse"*** oder eine ***„Monetarisierung von personenbezogenen Daten"*** durch Microsoft findet nicht statt.

Wir hoffen, Ihnen mit diesen Erläuterungen die Sicherheit vermitteln zu können, dass mit der Nutzung von Office 365 im schulischen oder im Unternehmensbereich keine unvertretbaren Sicherheits- oder Datenschutzrisiken verbunden sind. Selbstverständlich stehen Ihnen unsere Mitarbeiterinnen und Mitarbeiter jederzeit gern für weitere Gespräche zur Verfügung.

Mit freundlichen Grüßen

Thomas Langkabel
National Technology Officer
Microsoft Deutschland GmbH