Rechtsgrundlage für den Einsatz der Lern- und Kommunikationsplattform Office 365 an der

[bitte ergänzen: Universität/Hochschule]

gemäß DSGVO Art. 6(1)e

Laut Hochschulrahmengesetz HRG und den entsprechenden Landesgesetzen ist es vorrangige Aufgabe der Hochschulen,

- die Studierenden auf herausfordernde berufliche Tätigkeiten vorzubereiten, sie sozial zu fördern und weiterzubilden
- den wissenschaftlichen und künstlerischen Nachwuchs zu fördern
- ihr Personal weiterzubilden.

Um diese Aufgaben erfüllen zu können, muss die Hochschule personenbezogenen Daten der Beschäftigten und Studierenden verarbeiten. Dies geschieht heute grundsätzlich mit Hilfe von IT-Systemen, die eine effiziente wissenschaftliche Zusammenarbeit und adäquate Unterstützung der Verwaltungsvorgänge ermöglichen. IT-Systeme beinhalten aber auch Risiken, die potentiell einen unzulässigen Eingriff in die Grundrechte der Beschäftigten und Studierenden darstellen können.

In diesem Dokument wird dargelegt, dass die Verarbeitung personenbezogener Daten basierend auf der Lern- und Kommunikationsplattform Office 365 zur Wahrnehmung der gesetzlichen Aufgaben der Hochschule erforderlich ist und im öffentlichen Interesse liegt , weil nur das Minimum an Daten verarbeitet wird, das für die jeweilige Personengruppe erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten nicht überwiegen. Grundsätzlich stellt jegliche Verarbeitung personenbezogener Daten einen Eingriff in die Grundrechte dar, daher gehen wir hier auf den Zweck, die Art der gespeicherten Daten, den Ort der Speicherung, die Sicherheit und Integrität der Daten und der Schutz vor Identitätsdiebstahl, den Schutz der Privatsphäre, die Verfügbarkeit, die Vertraulichkeit, Nichtverkettung und das Widerspruchsrecht ein.

Eine Alternative zu IT-gestützter Kommunikation und Zusammenarbeit besteht nicht. Die Hochschule bietet eine Reihe von IT-Diensten an, die an unterschiedlichen Aufgaben angepasst sind. Zentraler Punkt bei allen Angeboten ist die Erfüllung der DSGVO: Schutz der Daten durch serverseitige Zertifizierungen oder Garantien, Recht auf Berichtigung, Recht auf Einschränkung bzw. Löschung und Recht auf Datenübertragbarkeit, soweit letztere dienstlich begründet ist.

Zweck der Verarbeitung

- IT-gestützte Zusammenarbeit der Mitarbeiter und Studierenden der Hochschule mittels der Microsoft Office 365 Dienste Exchange Online, Sharepoint Online und der Lernplattform Teams.
- Unterstützung von Hochschulen bei der Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben mit Hilfe von Microsoft Office365 zur Umsetzung des Bildungs- und Erziehungsauftrags, bei der Abwicklung der internen Aufgaben und Abläufe.

Name des eingesetzten Verfahrens und Dienstbeschreibungen

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

Art der gespeicherten Daten

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

Daten zu Dozenten und zum nichtwissenschaftlichen Personal:

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, E-Mailadresse, weitere dienstliche E-Mailadressen, Funktion, dienstliche Telefonnummer)
- Gruppenzugehörigkeiten in Teams, Mitbesitzer eines Teams, Lehrveranstaltungen

Daten der Studierenden:

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion)
- Studienrichtung
- Besuchte Lehrveranstaltungen, für die Teams eingerichtet werden
- Skripte, Übungen

Ort der Speicherung

- Es ist vertraglich gesichert, dass alle Nutzdaten nur innerhalb der EU in den Rechenzentren von Microsoft (derzeit Dublin und Amsterdam, in naher Zukunft auch 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 haben nur die dafür zugewiesenen und geschulten Mitarbeiter des Rechenzentrums

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 automatische oder manuelle Ende-zu-Ende Verschlüsselung aller E-Mails und Dokumente. Das Verfahren heißt Azure Information Protection und verschlüsselt Dokumente – je nach Voreinstellung durch die Systembetreuer im Rechenzentrum - automatisch oder mit einem Klick, sodass diese nur mehr von den voreingestellten Gruppen von Benutzern von Office 365 (Personalabteilung, Finanzabteilung, wissenschaftliche Kooperationspartner, usw) 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 sie können auch nur vom Benutzer selbst geändert werden.

Vertraulichkeit der Daten und Nichtverkettung

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.

Office 365 ermöglicht durch ein „Schutz gegen Datenverlust“ genanntes Regelwerk die strikte Trennung von vertraulichen Daten verschiedener Art. So kann z. B. die Finanzabteilung vertraulich Daten weder per E-Mail verschicken noch sie KollegInnen anderer Abteilungen freigeben.

Dieses Regelwerk verhindert eine beabsichtigte oder unbeabsichtigte Weitergabe von Daten, mit denen ein Profil eines Mitarbeiters oder Studierenden erzeugt werden könnte.

Schutz der Privatsphäre

Auf allen modernen Geräten laufen Office 365 Apps wie Onedrive oder Teams oder Outlook am Web in einem Isolationsmodus, sodass andere Apps keinen Zugriff auf diese Daten erhalten.

Intervenierbarkeit und Widerspruch

Jedes Mitglied der Hochschule 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 per dienstlicher E-Mail oder nach persönlicher Vorsprache an die Datenschutzstelle [**bitte angeben**] 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, 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	**Bitte anpassen:** **Das Hochschulnetzwerk ist durch eine Firewall geschützt. Die 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 Enterprise und durch Applikations- und Makro-Kontrolle geschützt.**
	Zugriffskontrolle	**Bitte anpassen:** **Die Benutzerkonten der Verwaltungs-mitarbeiter und Systembetreuer sind durch Multi-Faktor-Anmeldung oder biometrische Anmeldung gesichert.**
	Trennungskontrolle	Administrativer Zugriff auf die Office 365 Instanz der Hochschule ist auf die von der Hochschule 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 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 DS-GVO 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 allein Zugriff auf die Nutzdaten hat.

Rechtmäßigkeit der Verarbeitung

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 dienstlichen 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. Aus diesem Grund ist der Einsatz der Kommunikations- und Lernplattform Office 365 rechtmäßig.