KI:connect.NRW

Datenschutz-folgenabschätzung

für den Dienst „GPT“
in der Version 1.0 von 2024-04-19

Kommentiert [MP1]: Das Dokument enthält stellvertretende Einträge, z.B. das Logo im Dokumentenkopf oder Datumsangaben. Alle Stellen mit solchen Einträgen sind über Kommentare mit dem Text „Anpassen.“ markiert.

Auch in den übrigen Passagen kann sich Änderungsbedarf für die eigene Hochschule ergeben. Das Dokument sollte dann entsprechend angepasst werden.

Kommentiert [MP2]: Anpassen.

Generative KI
an Hochschulen in NRW

KI:connect.NRW

Datenschutz-Folgenabschätzung für den Dienst "GPT"

gemäß Art. 35 Abs. 1 DS-GVO

Fassung 1.0 von 2024-04-19

Kommentiert [MP3]: Anpassen.

1. Name und Anschrift der Verantwortlichen für die Datenverarbeitung

Verantwortlicher im Sinne des Art. 4 Nr. 7 EU-Datenschutz-Grundverordnung (DS-GVO) ist die/der Rektor/in / Präsident/in der Hochschule:

Rektor/in / Präsident/in der ###
Straße Hausnummer
PLZ Ort (Hausanschrift)
PLZ Ort (Postanschrift)
Deutschland
Telefon: +49 #### ##-######
Telefax: +49 #### ##-######
E-Mail: ###@###.de
Website: https://www.hochschule.de/

Die ### wird nachfolgend als „Hochschule“ bezeichnet.

Intern verantwortlich für den Betrieb ist das Rechenzentrum der Hochschule, im Folgenden „Rechenzentrum“. Das Rechenzentrum ist erreichbar unter:

Rechenzentrum der ###
Straße Hausnummer
PLZ Ort
E-Mail: ###@###.de

Kommentiert [MP4]: Anpassen.

Für bestimmte der verarbeiteten Daten findet eine Auftragsdatenverarbeitung durch Microsoft Ireland Operations Limited statt, im Folgenden „Microsoft“. Microsoft ist erreichbar unter:

Microsoft Ireland Operations Limited
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18 D18 P521

2. Name und Anschrift der Datenschutzbeauftragten der Hochschule

Stabsstelle Datenschutz der ###
Straße Hausnummer
PLZ Ort (Hausanschrift)
PLZ Ort (Postanschrift)
Deutschland
Telefon: +49 #### ##-######
Telefax: +49 #### ##-######
E-Mail: ###@###.de
Website: https://www.hochschule.de/

Kommentiert [MP5]: Anpassen.

3. Prozessbeschreibung

Name des Dienstes:	GPT, im Folgenden “Dienst”
Einsatzbereich und Zweck der Verarbeitungstätigkeit:	Der Dienst stellt Funktionen aus dem Bereich der generativen Künstlichen Intelligenz zur Verfügung. Darunter fällt die Möglichkeit der Generierung von Medien auf Basis menschlichen Inputs. Für die Nutzung des Dienstes werden personenbezogene Daten verarbeitet, um die nutzende Person zu authentifizieren.
Beginn der Verarbeitung:	Q#/20##
Zugriffsberechtigte Personen/Personengruppen:	Mitarbeiterinnen und Mitarbeiter der Hochschule
Art und Kategorien der personenbezogenen Daten:	Es werden (i) nicht-personenbezogene Daten sowie (ii) personenbezogene Daten gem. Art. 4 Abs. 1 DS-GVO verarbeitet.
Besondere Kategorien personenbezogener Daten gem. Art. 9, 10 DS-GVO:	Es werden keine besonderen personenbezogenen Daten Dritter gem. Art. 9 Abs. 1 DS-GVO bzw. Art. 10 DS-GVO verarbeitet.
Umfang der personenbezogenen Daten:	Der Umfang der Datensätze ist nutzungsabhängig. An den Dienst werden nur Daten von Personen übertragen, die sich aktiv gemäß der Nutzungsbedingungen für den Dienst authentifizieren.
Übermittlung der Daten an Dritte:	Es werden Daten gemäß dem Verzeichnis der Verarbeitungstätigkeiten übertragen.
Beschreibung der Übermittlungswege an Dritte:	Die Übermittlung der Daten an Microsoft erfolgt elektronisch und verschlüsselt.
Potentieller Zugriff auf die Daten durch Dritte:	Zugriffsberechtigt ist ausschließlich ausgewähltes Administrations- und Supportpersonal (i) des Rechenzentrums der Hochschule und (ii) von Microsoft.
Löschfristen:	Die Löschfristen sind dem Verzeichnis der Verarbeitungstätigkeiten zu entnehmen.
Rechtsgrundlage der Verarbeitung	Die Rechtsgrundlage der Verarbeitung ist der Datenschutzerklärung für den Dienst zu entnehmen.

Kommentiert [MP6]: Anpassen.

Kommentiert [MP7]: Anpassen.

Kommentiert [MP8]: Anpassen und ggf. Link setzen.

Kommentiert [MP9]: Anpassen und ggf. Link setzen.

Kommentiert [MP10]: Anpassen.

Kommentiert [MP11]: Anpassen und ggf. Link setzen.

Kommentiert [MP12]: Anpassen und ggf. Link setzen.

Wahrung der Informationspflichten ggü. Betroffenen	Die Wahrung der Informationspflichten ist der Datenschutzerklärung für den Dienst zu entnehmen.

Kommentiert [MP13]: Anpassen und ggf. Link setzen.

4. Einhaltung der Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO

Grundsatz	Ja	Nein	Weitere Informationen
Rechtmäßigkeit der Verarbeitung:	x		Weitere Informationen zur Einhaltung der Grundsätze der Datenverarbeitung sind den entsprechenden Dokumenten zu entnehmen: 1. Nutzungsbedingungen 2. Datenschutzerklärung 3. Verzeichnis der Verarbeitungstätigkeiten 4. Technische und organisatorische Maßnahmen (Rechenzentrum)
Verarbeitung nach Treu und Glauben:	x		
Transparenz:	x		
Datenminimierung:	x		
Richtigkeit:	x		
Speicherbegrenzung:	x		
Integrität und Vertraulichkeit:	x		
Anforderungen an Eignung technischer & organisatorischer Maßnahmen sind ausreichend und verhältnismäßig:	x		

Kommentiert [MP14]: Anpassen und ggf. Links setzen.

Kommentiert [MP15]: Anpassen.

5. Erläuterung zu Eintrittswahrscheinlichkeit und Schweregrad möglicher Schäden

Die Eintrittswahrscheinlichkeit für Schäden wird in vier Stufen eingeschätzt:

Grad	Bezeichnung	Eintrittswahrscheinlichkeit	
		Beschreibung	Beispiel
1	gering	Schaden kann auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	mittel	Schaden scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich, aber unwahrscheinlich.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	hoch	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.

4	sehr hoch	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich.	Befall durch Schadsoftware bei einem veralteten Betriebssystem ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

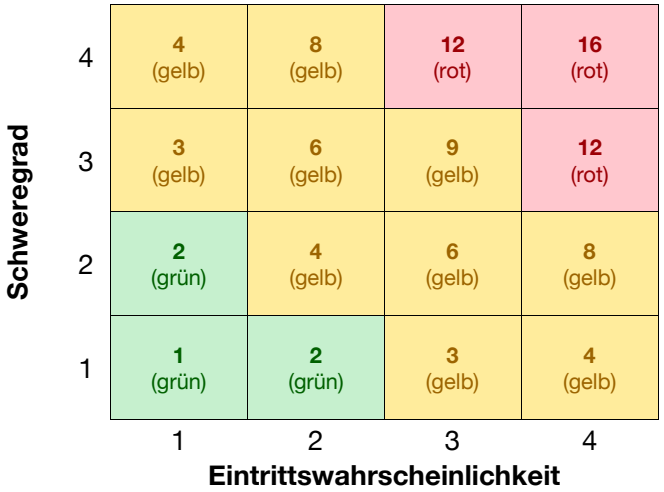
Der Schweregrad von Schäden wird in vier Intensitätsstufen klassifiziert:

Grad	Bezeichnung	Schweregrad der Schäden Beschreibung
1	gering	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
2	mittel	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
3	hoch	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
4	sehr hoch	Betroffene erleiden eventuell signifkante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Zur Risikoanalyse kann daraus ein Risikoindex wie folgt berechnet werden:

Risikoindex R = Eintrittswahrscheinlichkeit * Schweregrad

Daraus ergibt sich eine Risikomatrix für die Höhe des Risikoindex. Die Höhe des Risikoindex wird dazu in drei Bereiche eingeteilt:



Die drei Risikobereiche werden wie folgt benannt:

Index	Bezeichnung Risikoindex
1 - 2	geringe Schadenintensität (grün)
4 - 9	mittlere Schadenintensität (gelb)
10 - 16	hohe / sehr hohe Schadenintensität (rot)

6. Risikoanalyse

Die Hochschule verfolgt das Ziel, einen funktionalen, sicheren, benutzerfreundlichen und effizient zu nutzenden Dienst anzubieten. Die Verarbeitung personenbezogener Daten ist für den Betrieb des Dienstes unerlässlich, um Zugriffsrechte effektiv zu verwalten und eine personalisierte Nutzung zu ermöglichen.

Die Nutzenden erwarten einen sicheren Einsatz des Dienstes. Ihr Hauptinteresse liegt im Schutz ihrer personenbezogenen Daten vor unbefugtem Zugriff und Missbrauch. Sie legen Wert auf Datenschutz, die Integrität ihrer Daten und die Gewährleistung, dass ihre Informationen nur für den vorgesehenen Zweck verwendet werden.

Bei der Risikoanalyse ist zwischen zwei Nutzungsszenarien zu unterscheiden:

(1) Die Nutzenden halten die Nutzungsbedingungen für den Dienst ein und verstoßen nicht gegen diese sowie weitere Dienstvorschriften der Hochschule. Für dieses Szenario müssen alle Risikoindexe R maximal im gelben Bereich (i.e. $R \leq 9$).

(2) Die Nutzenden verstoßen gegen die Vorschriften, z.B. indem sie personenbezogene Daten oder andere unzulässige Inhalte als Teil ihrer Nutzung verarbeiten.

Kommentiert [MP16]: Anpassen und ggf. Link setzen.

Detailergebnisse der Risikoanalyse sind in den Anhängen A.1 bis A.3 wiedergegeben. Dabei sind Fälle gesondert markiert, denen eine unzulässige Nutzung im Sinne des Nutzungsszenarios (2) zugrunde liegt.

Bei der Verfügbarkeit des Dienstes (Anhang A.1) kommen als Schwachstellen sowohl der Ausfall von Geräten oder Systemen als auch allgemeine Datenverluste infrage. Für die beschriebenen Risikoszenarien liegt der Risikoindex im niedrigen bis mittleren Bereich. Eine Reduzierung der Schadenintensität im Falle mittlerer Risikoindexe ist durch Backups bzw. die Nutzung alternativer Endgeräte möglich und vorgesehen.

Beim Schutz der verarbeiteten Daten geht es sowohl um den Abfluss von Informationen an Unbefugte als auch um die Gefahr des Identitätsdiebstahls (Anhang A.2) Für die beschriebenen Risikoszenarien liegt der Risikoindex meist im mittleren Bereich. Eine Reduzierung der Schadenintensität ist jeweils durch geeignete Maßnahmen möglich. Hohe Risikoindexe ergeben sich lediglich bei unzulässiger Nutzung, wenn

vorschriftswidrig vertrauliche oder streng vertrauliche Daten mit oder ohne Personenbezug in den Dienst eingegeben werden. Die Reduzierung der Schadenintensität soll durch Schulung und Sensibilisierung des an der Nutzung beteiligten Personals erfolgen.

Bei der Integrität der verarbeiteten Daten bestehen Schwachstellen im beabsichtigten oder unbeabsichtigten Verändern von Daten durch Personen oder Softwarefehler (Anhang A.3). Für die beschriebenen Risikoszenarien liegen Risikoindexe überwiegend im mittleren Bereich. Eine Reduzierung der Schadenintensität ist jeweils durch geeignete Maßnahmen möglich. Hohe Risikoindexe zeigen sich vor allem bei den Nutzenden bzw. ihren Endgeräten. Die Reduzierung der Schadenintensität soll durch Maßnahmen wie Verschlüsselung, Multifaktor-Authentifizierung (MFA) sowie durch Schulung und Sensibilisierung erfolgen.

7. Ergebnis

Prüfpunkt	Ja	Nein
Geeignetheit: Der gewünschte Zweck ist mit dem zu bewertenden Prozess erreichbar.	x	
Erforderlichkeit: Es gibt kein milderes Mittel, das denselben Zweck unter ähnlichem Aufwand herbeiführen würde.	x	
Verhältnismäßigkeit: Der Eingriff in das Schutzgut des Betroffenen ist verhältnismäßig zum verfolgten Zweck.	x	
Berechtigte Interessen des Verantwortlichen überwiegen	x	

Die Abwägung ergibt, dass die Interessen der Nutzenden bezüglich des Datenschutzes und die Interessen des Anbieters an der Bereitstellung einer sicheren, effizienten Software in angemessener Weise berücksichtigt und abgewogen werden. Die Datenverarbeitung ist auf das notwendige Maß beschränkt, und durch die getroffenen Sicherheitsmaßnahmen wird sichergestellt, dass das Risiko für die Nutzenden minimal ist.

Das Risiko eines Datenschutzvorfalls ist vertretbar und im Falle eines solchen Vorfalls ist die Schadenintensität überwiegend niedrig bis mittel. Dies führt zu dem Schluss, dass die Datenverarbeitung in einem angemessenen Gleichgewicht zwischen den Interessen der Nutzenden und der Hochschule gewahrt wird.

Der Verarbeitungsprozess geschieht rechtmäßig unter Einhaltung der Verarbeitungsgrundsätze. Er ist notwendig und verhältnismäßig. Der Prozess kann in Betrieb genommen werden.

Anhang A.1 Risikoanalyse zur Verfügbarkeit des Dienstes

ID	Schwachstelle	Risikoquelle	Risikoszenario	Eintrittswahrscheinlichkeit	Grad	Schwergrad des Schadens	Grad	Risikoindex	Maßnahmen	Risikoindex nach Maßnahmen und Begründung	
1	Ausfall von Geräten oder Systemen	IT Systeme Microsoft Cloud, aber auch Schnittstellensysteme, die eine Web-Oberfläche oder einen Webservice anbieten (z.B. office.com)	Die IT Systeme von Microsoft sind temporär nicht mehr erreichbar oder fallen aus, z.B. durch Hackerangriff, Fehler im Cloud Rechenzentrum von Microsoft	Szenario kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	2	Der Dienst kann nicht verwendet werden	1	2 (grün)	Vorhalten von Alternativen	1 (grün)	Geringere Eintrittswahrscheinlichkeit, da Alternativen Verwendung anderer, u.U. an der Hochschule gehosteter KI-Systeme ermöglichen
2	Ausfall von Geräten oder Systemen	IT Systeme der Hochschule , Schnittstellensysteme, die eine Web-Oberfläche oder einen Webservice anbieten (z.B. SSO der Hochschule)	Die zur Cloud gehörenden IT-Systeme der Hochschule sind temporär nicht mehr erreichbar oder fallen aus, z.B. aufgrund eines Hackerangriffs, fehlerhafter Updates, Fehler in der Administration.	Szenario kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	2	Der Dienst kann nicht verwendet werden	1	2 (grün)	Vorhalten von Alternativen	1 (grün)	Geringere Eintrittswahrscheinlichkeit, da Alternativen Verwendung anderer, u.U. an der Hochschule gehosteter KI-Systeme ermöglichen
3	Ausfall von Geräten oder Systemen	Netzwerkverbindung (DFN, Hochschule, lokaler Anbieter im HomeOffice)	Aufgrund einer Störung kommt es zu einem Ausfall der Internetverbindung	Szenario kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	2	Der Dienst kann nicht verwendet werden	1	2 (grün)		2 (grün)	
4	Ausfall von Geräten oder Systemen	IT Systeme (Endgeräte) der Nutzenden bzw. der Nutzende	Defekt bzw. Problem beim Nutzenden, weder Hochschul-Systeme noch Microsoftsysteme sind erreichbar.	Risiko kann eintreten und ist von dem Nutzenden abhängig	3	Der Dienst kann nicht verwendet werden	1	3 (gelb)	Nutzung alternatives Endgerät	2 (grün)	Geringere Eintrittswahrscheinlichkeit, da alternative Endgeräte Weiter-Verwendung des Dienstes ermöglichen
5	Datenverlust	IT Systeme (Endgeräte) der Nutzenden bzw. der Nutzende, Hacker	Gezielter Angriff auf Mitarbeitenden der Hochschule (z.B. Phishing) Durch den kompromittierten Account werden Daten gelöscht oder nicht mehr verfügbar gemacht.	Hackerangriffe sind sehr wahrscheinlich bzw. werden weiter zunehmen.	3	Unbefugter Zugriff auf Informationen	1	3 (gelb)	Redundante Speicherung von Daten in den IT Systemen der Hochschule	2 (grün)	Geringerer Schweregrad, da gelöschte oder nicht mehr verfügbare Daten wieder-hergestellt werden können
6	Datenverlust	IT Systeme Microsoft	Die IT Systeme von Microsoft fallen aus und die dort gespeicherten Informationen gehen verloren.	Nach bisherigen Erfahrungen nicht aufgetreten	2	Unbefugter Zugriff auf Informationen	1	2 (grün)	Redundante Speicherung von Daten in den IT Systemen der Hochschule	1 (grün)	Geringerer Schweregrad, da gelöschte oder nicht mehr verfügbare Daten wieder-hergestellt werden können
7	Datenverlust	IT Systeme der Hochschule (der Cloud zugeordnet)	Die zur Cloud gehörenden IT-Systeme der Hochschule fallen aus und die dort gespeicherten Daten gehen verloren.	Nach bisherigen Erfahrungen nicht aufgetreten	2	Für die Dauer des Ausfalls ist kein Zugriff auf die Online-Daten möglich.	2	4 (gelb)	Backup IT Systeme der Hochschule	2 (grün)	Geringerer Schweregrad, da ein Ausfall zeitnah kompensiert werden kann
8	Datenverlust	IT Systeme (Endgeräte) der Nutzenden bzw.der Nutzende	Defekt bzw. Problem beim Nutzenden, z.B. Datenverlust durch defekte Festplatte.	Anzahl der verschiedenen, dezentral oder garnicht verwalteten Endgeräte macht das Eintreten wahrscheinlich	3	Daten die in der Cloud gespeichert wurden sind vom Ausfall nicht betroffen. Zugriff über anderes Endgerät möglich.	1	3 (gelb)	Redundante Speicherung von Daten in den IT Systemen der Hochschule	2 (grün)	Geringerer Schweregrad, da gelöschte oder nicht mehr verfügbare Daten wieder-hergestellt werden können

Anhang A.2 Risikoanalyse zum Schutz der Daten

ID	Schwachstelle	Risikoquelle	Risikoszenario	Differenzierungsmerkmal	Eintrittswahrscheinlichkeit	Grad	Schwergrad des Schadens	Grad	Risikoindex	Maßnahmen	Risikoindex nach Maßnahmen und Begründung	
1	Informationsabfluss (Zugriff auf Daten durch Dritte oder Social Engineering)	IT Systeme Microsoft	Zugriff auf Informationen durch Personal von Microsoft	Datenkategorie: öffentlich	Zugriff technisch möglich	3	Daten sind ohnehin öffentlich	1	3 (gelb)	AV Vertrag Microsoft	2 (grün)	Geringere Eintrittswahrscheinlichkeit für Zugriff
				Datenkategorie: intern, ohne Personenbezug	Zugriff technisch möglich	3	Unbefugter Zugriff auf Informationen	2	6 (gelb)	AV Vertrag Microsoft	4 (gelb)	Geringere Eintrittswahrscheinlichkeit für Zugriff
				Datenkategorie: vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	3	Unbefugter Zugriff auf Informationen	3	9 (gelb)	AV Vertrag Microsoft, Nutzungsbedingungen, Schulung und Sensibilisierung	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für Zugriff und für Verstöße gegen Nutzungsbedingungen
				Datenkategorie: streng vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	3	Unbefugter Zugriff auf Informationen	4	12 (rot)	AV Vertrag Microsoft, Nutzungsbedingungen, Schulung und Sensibilisierung	8 (gelb)	Geringere Eintrittswahrscheinlichkeit für Zugriff und für Verstöße gegen Nutzungsbedingungen
2	Informationsabfluss	IT Systeme der Hochschule, IT Center Personal	ITC Mitarbeitende erhalten Zugriff auf den Tenant auch wenn die Berechtigung erloschen ist (z.B. durch veraltete Konfiguration; Betrifft nur den Fall, dass der Mitarbeitende in der Hochschule verweilt)	Datenkategorie: öffentlich	Möglich z.B. bei Nichtbeachtung Prozess "Mitarbeitende kommen/gehen"	3	Daten sind ohnehin öffentlich	1	3 (gelb)	–	3 (gelb)	–
				Datenkategorie: intern, ohne Personenbezug	Möglich z.B. bei Nichtbeachtung Prozess "Mitarbeitende kommen/gehen"	3	Unbefugter Zugriff auf Informationen	2	6 (gelb)	Monitoring Admin Zugänge	4 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
				Datenkategorie: vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	3	Unbefugter Zugriff auf Informationen	3	9 (gelb)	Monitoring Admin Zugänge, Schulung und Sensibilisierung, Nutzungsbedingungen	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler und für Verstöße gegen Nutzungsbedingungen
				Datenkategorie: streng vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	3	Unbefugter Zugriff auf Informationen	4	12 (rot)	Monitoring Admin Zugänge, Schulung und Sensibilisierung, Nutzungsbedingungen	8 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler und für Verstöße gegen Nutzungsbedingungen
3	Informationsabfluss	IT Systeme der Hochschule, IT Center Personal	Ehemalige Mitarbeitende können nach Ausscheiden aus der Hochschule auf ihre (geteilten) Daten zugreifen	Datenkategorie: öffentlich	Möglich bei technischer Störung im Lifecycle der IdM Accounts	2	Daten sind ohnehin öffentlich	1	2 (grün)	–	2 (grün)	–
				Datenkategorie: intern, ohne Personenbezug	Möglich bei technischer Störung im Lifecycle der IdM Accounts	2	Unbefugter Zugriff auf Informationen	2	4 (gelb)	Automatischer Entzug	2 (grün)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
				Datenkategorie: vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	2	Unbefugter Zugriff auf Informationen	3	6 (gelb)	Automatischer Entzug, Schulung und Sensibilisierung, Nutzungsbedingungen	3 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler und für Verstöße gegen Nutzungsbedingungen
				Datenkategorie: streng vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	Automatischer Entzug, Schulung und Sensibilisierung, Nutzungsbedingungen	4 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler und für Verstöße gegen Nutzungsbedingungen

ID	Schwachstelle	Risikoquelle	Risikoszenario	Differenzierungsmerkmal	Eintrittswahrscheinlichkeit	Grad	Schwergrad des Schadens	Grad	Risikoindex	Maßnahmen	Risikoindex nach Maßnahmen und Begründung	
4	Informationsabfluss	IT Systeme der Hochschule, IT Center Personal	Hochschul-Mitarbeitende können unbefugt auf personenbezogene Daten anderer Hochschul-Mitarbeitenden zugreifen (z..B. durch Fehler nach einem Update)	Datenkategorie: öffentlich	Möglich bei Konfigurationsfehlern, z.B. durch fehlerhafte Updates der Software oder manuelle Fehler	2	Daten sind ohnehin öffentlich	1	2 (grün)	–	2 (grün)	–
				Datenkategorie: intern, ohne Personenbezug	Möglich bei Konfigurationsfehlern, z.B. durch fehlerhafte Updates der Software oder manuelle Fehler	2	Unbefugter Zugriff auf Informationen	2	4 (gelb)	Software Audits	2 (grün)	Geringere Eintrittswahrscheinlichkeit für technische Fehler
				Datenkategorie: vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	2	Unbefugter Zugriff auf Informationen	3	6 (gelb)	Software Audits	3 (gelb)	Geringere Eintrittswahrscheinlichkeit für technische Fehler
				Datenkategorie: streng vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	Software Audits	4 (gelb)	Geringere Eintrittswahrscheinlichkeit für technische Fehler
5	Informationsabfluss	Nutzende	Fehlerhafte Freigaben durch Nutzende	Datenkategorie: öffentlich	Möglich bei falschen Freigaben durch fehlerhafte Bedienung	3	Daten sind ohnehin öffentlich	1	3 (gelb)	–	3 (gelb)	–
				Datenkategorie: intern, ohne Personenbezug	Möglich bei falschen Freigaben durch fehlerhafte Bedienung	3	Unbefugter Zugriff auf Informationen	2	6 (gelb)	Audit über öffentliche Daten, Schulung und Sensibilisierung	4 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
				Datenkategorie: vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	3	Unbefugter Zugriff auf Informationen	3	9 (gelb)	Audit über öffentliche Daten, Schulung und Sensibilisierung	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
				Datenkategorie: streng vertraulich und/oder mit Personenbezug	Hinweis: Datenkategorie darf gem. Nutzungsbedingungen nicht verwendet werden.	3	Unbefugter Zugriff auf Informationen	4	12 (rot)	Audit über öffentliche Daten, Schulung und Sensibilisierung	8 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
6	Informationsabfluss	Behörden, Netzanbieter	Zugriff auf Daten, z.B. durch Mithören der Kommunikation	Datenkategorie: alle	Zugriff technisch möglich	3	Unbefugter Zugriff auf Informationen	3	9 (gelb)	Speicherung von Daten nur in den IT Systemen der Hochschule	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für Zugriff Dritter
7	Informationsabfluss	US-Amerikanische Behörden und Geheimdienste	Zugriff auf Daten im Rahmen der rechtlichen Regelungen der USA	Datenkategorie: alle	Zugriff technisch möglich	3	Unbefugter Zugriff auf Informationen	3	9 (gelb)	Microsoft Maßnahmen zur Rechtseinhaltung	3 (gelb)	Erheblich geringere Eintrittswahrscheinlichkeit für Zugriff Dritter
8	Informationsabfluss	Hacker	Direkter Angriff auf IT-Systeme und Netzkomponenten (z.B. Systeme, die nicht gepatcht bzw. nicht gehärtet sind; Mithören der Kommunikation)	Systeme: Microsoft	Angriff technisch möglich und wahrscheinlich.	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	AV Vertrag und Policy MS	4 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
				Systeme: Hochschule	Angriff technisch möglich und wahrscheinlich.	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	Verschlüsselung, Schwachstellenmanagement, MFA	4 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
				Systeme Mitarbeitende (dienstlich)	Angriff technisch möglich und wahrscheinlich.	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	Verschlüsselung, Schwach-stellenmanagement, MFA, Schulung und Sensibilisierung	4 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
				Systeme Mitarbeitende (privat)	Angriff technisch möglich und wahrscheinlich.	3	Unbefugter Zugriff auf Informationen	3	9 (gelb)	Verschlüsselung, MFA, Schulung und Sensibilisierung	6 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
9	Identitätsdiebstahl bzw. Missbrauch von Accounts	End-Point-Security bei Personal	Durch Nutzung von Phishing, Viren, etc. werden Informationen zur Authentifizierung abgegriffen.	Personengruppe: Cloud Administratoren Microsoft	Aufgrund gemachter Erfahrungen bzw. der gegebenen Umstände ist der Eintritt unwahrscheinlich	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	AV Vertrag und Policy MS	4 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
				Personengruppe: Cloud Administratoren der Hochschule	Aufgrund gemachter Erfahrungen bzw. der gegebenen Umstände ist der Eintritt unwahrscheinlich	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	Verschlüsselung, Schwachstellenmanagement, MFA	4 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
				Personengruppe: IT Admins der Einrichtungen	Aufgrund gemachter Erfahrungen bzw. der gegebenen Umstände ist der Eintritt unwahrscheinlich	2	Unbefugter Zugriff auf Informationen	4	8 (gelb)	Verschlüsselung, Schwach-stellenmanagement, MFA, Schulung und Sensibilisierung	4 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
				Personengruppe: Mitarbeitende	Angriff technisch möglich und wahrscheinlich.	3	Unbefugter Zugriff auf Informationen	4	12 (rot)	Verschlüsselung, MFA, Schulung und Sensibilisierung	8 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken

Anhang A.3 Risikoanalyse zur Integrität der Daten

ID	Schwachstelle	Risikoquelle	Risikoszenario	Differenzierungsmerkmal	Eintrittswahrscheinlichkeit	Grad	Schwergrad des Schadens	Grad	Risikoindex	Maßnahmen	Risikoindex nach Maßnahmen und Begründung	
1	Mitarbeitende haben Schreibzugriff auf Daten (beabsichtigt oder unbeabsichtigt)	Microsoft	Daten werden fehlerhaft oder unzulässig verändert	Datenverarbeitende Systeme: alle	Aufgrund gemachter Erfahrungen bzw. der gegebenen Umstände ist der Eintritt unwahrscheinlich	3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	AV Vertrag und Policy Microsoft	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für Zugriff
		IT Center				3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	–	6 (gelb)	–
		IT Admins				3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	Schulung und Sensibilisierung	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
		Nutzende				3	Unbefugter Schreibzugriff auf Informationen	4	12 (rot)	Schulung und Sensibilisierung	8 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative und Nutzungsfehler
2	System-/ Programmfehler beim Schreibzugriff auf Daten	Microsoft	Daten werden fehlerhaft oder unvollständig übertragen oder gespeichert	Datenverarbeitende Systeme: alle	Aufgrund gemachter Erfahrungen bzw. der gegebenen Umstände ist der Eintritt unwahrscheinlich	3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	AV Vertrag und Policy Microsoft	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für Zugriff
		IT Center				3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	Software Audits	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
		Endgeräte				3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	Schulung und Sensibilisierung	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für administrative Fehler
3	Unbefugte Personen haben Schreibzugriff auf Daten	Hacker	Daten werden auf dem Transportweg unzulässig verändert	Datenverarbeitende Systeme: alle	Aufgrund gemachter Erfahrungen bzw. der gegebenen Umstände ist der Eintritt unwahrscheinlich	3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	Verschlüsselung des Übertragungsweges	6 (gelb)	Geringere Erfolgswahrscheinlichkeit für Intrusionstechniken
4	Unbefugte Personen haben Schreibzugriff auf Daten	Hacker	Daten werden auf Endgeräten unzulässig verändert	Datenverarbeitende Systeme: Microsoft	Aufgrund gemachter Erfahrungen bzw. der gegebenen Umstände ist der Eintritt unwahrscheinlich	2	Unbefugter Schreibzugriff auf Informationen	3	6 (gelb)	AV Vertrag und Policy Microsoft	3 (gelb)	Geringere Eintrittswahrscheinlichkeit für Zugriff
				Datenverarbeitende Systeme: Hochschule		3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	Verschlüsselung, Schwachstellenmanagement, MFA	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für Intrusionstechniken und administrative Fehler
				Datenverarbeitende Systeme: Mitarbeitende (dienstlich)		3	Unbefugter Schreibzugriff auf Informationen	3	9 (gelb)	Verschlüsselung, Schwachstellenmanagement, MFA, Schulung und Sensibilisierung	6 (gelb)	Geringere Eintrittswahrscheinlichkeit für Intrusionstechniken und administrative Fehler
				Datenverarbeitende Systeme: Mitarbeitende (privat)		4	Unbefugter Schreibzugriff auf Informationen	3	12 (rot)	Verschlüsselung, MFA, Schulung und Sensibilisierung	9 (gelb)	Geringere Eintrittswahrscheinlichkeit für Intrusionstechniken und Nutzungsfehler