

reuschlaw

# Vorlage für eine Datenschutz- Folgenabschätzung

zum Einsatz von Microsoft 365 durch öffentliche Bildungseinrichtungen

RA Stefan Hessel, LL.M.; RAin Christina Kiefer, LL.M.  
Stand: 30.01.2023

## Vorbemerkung

Diese Vorlage soll eine Hilfestellung für die Umsetzung der datenschutzrechtlichen Anforderungen an den Einsatz von Microsoft 365 durch öffentliche Bildungseinrichtungen geben. Öffentliche Bildungseinrichtungen, die Microsoft 365 einsetzen, sind in der Regel selbst für die Umsetzung der datenschutzrechtlichen Anforderungen verantwortlich. Ihnen obliegt die Pflicht, nach Art. 35 DSGVO zu prüfen, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist, und diese ggf. durchzuführen. Mithilfe der Vorlage können die datenschutzrechtlichen Risiken des Einsatzes von Microsoft 365 im Einzelfall bewertet und dokumentiert werden. Im Ergebnis kann der Einsatz von Microsoft 365 an einer öffentlichen Bildungseinrichtung im Einzelfall datenschutzrechtlich zulässig sein, wenn eine geeignete Auswahl risikoverringender technischer und organisatorischer Maßnahmen umgesetzt wird.

Diese Vorlage stellt keine rechtliche Beratung zum Einsatz von Microsoft 365 durch öffentliche Bildungseinrichtungen dar und ersetzt diese auch nicht. Die Vorlage dient lediglich als Hilfestellung für die Durchführung einer Datenschutz-Folgenabschätzung und wird ohne Gewähr auf Vollständigkeit zur Verfügung gestellt. Es obliegt dem Verantwortlichen, die Vorlage auf den Einzelfall und die konkreten Gegebenheiten anzupassen. Hierbei ist insbesondere eine eigene Würdigung aller Umstände des Einzelfalls unter Berücksichtigung der aktuellen Rechtslage vorzunehmen. Es wird ausdrücklich darauf hingewiesen, dass sich durch eine geänderte Rechtslage die Notwendigkeit zur Anpassung der Vorlage ergeben kann.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung-Nicht kommerziell 4.0 International Lizenz](https://creativecommons.org/licenses/by-nc/4.0/).

Melden Sie sich jederzeit gerne, wenn Sie unsere Unterstützung für einen datenschutzkonformen Einsatz von Microsoft 365 benötigen oder Fragen haben. Gerne erläutern wir Ihnen unser Vorgehen ausführlich in einem persönlichen Gespräch.

T > + 49 681 / 859 160 0

E > [info@reuschlaw.de](mailto:info@reuschlaw.de)

[www.reuschlaw.de](http://www.reuschlaw.de)

# Inhalt

1	Einleitung .....	3
1.1	Was ist eine Datenschutz-Folgenabschätzung? .....	3
1.2	Wann ist eine Datenschutz-Folgenabschätzung erforderlich? .....	3
2	Vorlage für eine Datenschutzfolgenabschätzung .....	5
2.1	Systematische Beschreibung der Verarbeitung (Art. 35 Abs. 7 lit. a) DSGVO) .....	5
2.1.1	Stammdaten der Einrichtung .....	5
2.1.2	Abkürzungsverzeichnis .....	6
2.1.3	Notwendigkeit der DSFA .....	7
2.1.4	Prüfgegenstand der DSFA .....	8
2.1.5	Verarbeitung personenbezogener Daten .....	11
2.1.6	Beschreibung der Nutzungsszenarien .....	15
2.1.7	Verantwortliche für die Verarbeitung .....	16
2.1.8	Rechtsgrundlagen.....	18
2.1.9	Drittlandsübermittlung.....	22
2.1.10	Gewährleistung der Betroffenenrechte .....	24
2.1.11	Löschung der Daten .....	25
2.2	Notwendigkeit und Verhältnismäßigkeit der Verarbeitung (Art. 35 Abs. 7 lit. b) DSGVO) .....	26
2.3	Risikoanalyse (Art. 35 Abs. 7 lit. c) DSGVO).....	28
2.3.1	Risiken bei Einsatz von Microsoft 365 an der [ <i>Name der öffentlichen Bildungseinrichtung</i> ] 30	
2.3.2	Gesamtrisiko.....	32
2.4	Ermittlung und Bewertung von Abhilfemaßnahmen (Art. 35 Abs. 7 lit. d) DSGVO).....	33
2.4.1	Abhilfemaßnahmen zu den ermittelten Risiken.....	33
2.4.2	Abschließende Risikoanalyse unter Berücksichtigung der Abhilfemaßnahmen .....	35
2.5	Weitere Inhalte.....	36
2.5.1	Nachhaltige Sicherung des Datenschutzes (Art. 35 Abs. 11 DSGVO) .....	36
2.5.2	Anlagen.....	36

# 1 Einleitung

## 1.1 Was ist eine Datenschutz-Folgenabschätzung?

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein zentraler Bestandteil der Datenschutz-Compliance bei dem Einsatz von Microsoft 365. Nach Art. 35 Abs. 1 Datenschutz-Grundverordnung (DSGVO) ist ein Verantwortlicher zur Durchführung einer DSFA verpflichtet, soweit aufgrund des Umfangs, Kontexts oder Zwecks der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Ist dies der Fall, hat der Verantwortliche vor Beginn der Verarbeitung alle Verarbeitungsprozesse zu analysieren, deren rechtliche Zulässigkeit zu begutachten sowie die mit der Verarbeitung verbundenen Risiken zu ermitteln und geeignete Abhilfemaßnahmen zu ergreifen. Die Durchführung der DSFA ist hinreichend zu dokumentieren.

Gemäß Art. 35 Abs. 7 DSGVO beinhaltet eine DSFA mindestens die folgenden Punkte:

- eine Beschreibung der Verarbeitungsvorgänge sowie der Verarbeitungszwecke;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen;
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen.

## 1.2 Wann ist eine Datenschutz-Folgenabschätzung erforderlich?

Eine DSFA ist erforderlich, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Wie das Risiko zu ermitteln, ist in der DSGVO nicht ausdrücklich festgelegt. Die Datenschutzkonferenz (DSK) definiert das Risiko in ihrem [Kurzpapier Nr. 18](#) als *„das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder das zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann“*. Folglich sind bei der Ermittlung des Risikos zum einen die Schwere des Schadens und zum anderen die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten, zu berücksichtigen.

Darüber hinaus sind in Art. 35 Abs. 3 DSGVO einige Regelbeispiele aufgeführt, bei deren Vorliegen eine DSFA in jedem Fall erforderlich ist. Zur weiteren Konkretisierung haben die Datenschutzaufsichtsbehörden des [Bundes](#) und der Länder (z.B. [der Landesbeauftragte für](#)

[Datenschutz und Informationsfreiheit \(LfDI\) Baden-Württemberg](#)) sog. „Muss-Listen“ für den öffentlichen Bereich veröffentlicht, in denen Verarbeitungsvorgänge benannt werden, für die in jedem Fall eine DSFA durchzuführen ist. Von der Möglichkeit, Verarbeitungsvorgänge festzulegen, die keiner DSFA bedürfen, haben die Datenschutzaufsichtsbehörden bislang keinen Gebrauch gemacht. Neben den genannten speziellen Vorgaben ist die Erforderlichkeit einer DSFA zudem nach den allgemeinen Kriterien des Art. 35 Abs. 1 DSGVO und damit nach den Umständen des Einzelfalls zu bewerten. Hierfür können die [Kriterien der Leitlinien WP 248 Rev.01 der Artikel-29-Datenschutzgruppe](#) (WP29) herangezogen werden.

Wir empfehlen für den Einsatz von Microsoft 365 durch öffentliche Bildungseinrichtungen in jedem Fall eine DSFA durchzuführen, da Verantwortliche unserer Erfahrung nach auf diesem Wege eine datenschutzkonforme Nutzung sicherstellen und hinreichend dokumentieren können. Unabhängig von der Durchführung einer DSFA sind Verantwortliche nach Art. 5 Abs. 2, 24, 25, 32 DSGVO dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zum Datenschutz zu treffen und den Nachweis erbringen zu können, dass die Vorschriften der DSGVO gewahrt werden. Diese Rechenschaftspflicht kann mit der Durchführung einer DSFA miterfüllt werden.

## 2 Vorlage für eine Datenschutzfolgenabschätzung

### 2.1 Systematische Beschreibung der Verarbeitung (Art. 35 Abs. 7 lit. a) DSGVO)

Hinweis: Nach Art. 35 Abs. 7 lit. a) DSGVO hat eine DSFA in jedem Fall eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen, zu beinhalten. Wir empfehlen für eine systematische Beschreibung der Verarbeitung zumindest auf die folgenden Punkte einzugehen, die in den kommenden Abschnitten näher erläutert werden:

- Stammdaten der Einrichtung;
- Notwendigkeit der DSFA;
- Prüfgegenstand der DSFA;
- Beschreibung der Verarbeitung im Allgemeinen;
- Beschreibung der konkreten Nutzungsszenarien;
- datenschutzrechtliche Verantwortlichkeiten;
- Rechtsgrundlagen der Datenverarbeitung, auch im Hinblick auf etwaige Drittlandsübermittlungen;
- weitere datenschutzrechtliche Anforderungen, wie z.B. die Gewährleistung der Betroffenenrechte oder die Löschung der Daten.

#### 2.1.1 Stammdaten der Einrichtung

Die Stammdaten der [Name der öffentlichen Bildungseinrichtung] lauten wie folgt:

Namen und die Kontaktdaten der/des Verantwortlichen:

Name / Bezeichnung der datenverarbeitenden Stelle	XXX
Name der Einrichtungsleitung	XXX
Adresse	XXX
Telefon	XXX

(*Sofern vorhanden:*) Angaben zur Leitung der Datenverarbeitung:

Name	XXX
------	-----

Adresse	XXX
Telefon	XXX
E-Mail-Adresse	XXX

(Sofern vorhanden:) Angaben zur Person der/des Datenschutzbeauftragten:

Name	XXX
Adresse	XXX
Telefon	XXX
E-Mail-Adresse	XXX

### 2.1.2 Abkürzungsverzeichnis

Abkürzung	Bedeutung
BDSG	Bundesdatenschutzgesetz
DPA	Data Protection Addendum (als englische Übersetzung für den Datenschutznachtrag zu den Produkten und Services von Microsoft)
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
EO	Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities
EU Data Boundary	EU Data Boundary for the Microsoft Cloud (auf Deutsch „EU-Datengrenze für die Microsoft Cloud“)
EuGH	Europäischer Gerichtshof
EU-Kommission	Europäische Kommission
EWR	Europäischer Wirtschaftsraum
GG	Grundgesetz
LDSG	Landesdatenschutzgesetz
Microsoft Irland	Microsoft Ireland Operations Limited
SCC	Standard Contractual Clauses (auf Deutsch „Standardvertragsklauseln“)
WP29	Artikel-29-Datenschutzgruppe

### 2.1.3 Notwendigkeit der DSFA

Hinweis: Gemäß Art. 35 Abs. 1 DSGVO besteht die Pflicht zur Durchführung einer DSFA, soweit aufgrund des Umfangs, Kontexts oder Zwecks der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Das Risiko ist in der DSGVO nicht legaldefiniert, sodass die Definition der DSK aus ihrem [Kurzpapier Nr. 18](#) als Hilfestellung herangezogen werden sollte. Folglich sind die Schwere des Schadens und die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten, zu berücksichtigen.

Darüber hinaus gilt es, Folgendes zu beachten:

- **Art. 35 Abs. 3 DSGVO** beinhaltet **Regelbeispiele** für die Fälle, in denen eine DSFA in jedem Fall erforderlich ist (systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen; umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO; systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche).
- Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben gemäß **Art. 35 Abs. 4 DSGVO** eine sog. „**Muss-Liste**“ für den öffentlichen Bereich veröffentlicht,<sup>1</sup> in der Datenverarbeitungsvorgänge benannt werden, für die in jedem Fall eine DSFA durchzuführen ist.
- Nach **Art. 35 Abs. 5 DSGVO** können die Datenschutzaufsichtsbehörden auch eine Liste von Verarbeitungsvorgängen erstellen, für die keine DSFA erforderlich ist. Eine solche Negativliste haben die Datenschutzbehörden jedoch bis dato nicht veröffentlicht.
- Da die Muss-Liste der Datenschutzaufsichtsbehörden nicht abschließend ist, ist die Frage der Notwendigkeit der Durchführung einer DSFA beim Einsatz von Microsoft 365 an einer öffentlichen Bildungseinrichtung stets auch nach den allgemeinen Kriterien des **Art. 35 Abs. 1 und 3 DSGVO** anhand der **Umstände des Einzelfalls** zu beurteilen.<sup>2</sup>

---

<sup>1</sup> Siehe z.B.: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), [Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes](#), zuletzt abgerufen: 30.01.2023.

<sup>2</sup> Siehe Hansen in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed., Stand: 01.11.2021, Art. 35 DS-GVO, Rn. 25.

Zur Beurteilung des Risikos für die Rechte und Freiheiten der Betroffenen sollten insbesondere die [Kriterien der WP29](#) berücksichtigt werden.

Ob für den Einsatz von Microsoft 365 an einer öffentlichen Bildungseinrichtung eine DSFA durchgeführt werden muss, hängt vom Einzelfall ab. Sofern z.B. im Rahmen des Einsatzes von Microsoft 365 eine umfangreiche Datenverarbeitung stattfindet, die insbesondere auch Daten von besonders schutzbedürftigen Betroffenen, wie etwa Minderjährigen, umfasst, dürfte in der Regel ein hohes Risiko für die Rechte und Freiheiten der Betroffenen bestehen. Gleiches wird in der Regel für Fälle gelten, in denen Profile und Prognosen zur Ausbildungs- oder Arbeitsleistung von Betroffenen gebildet werden können. Es sind jedoch auch Fälle denkbar, in denen aufgrund der konkreten Umstände der Verarbeitung kein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht und damit eine DSFA nicht zwingend erforderlich ist. Ein Beispiel hierfür kann der Einsatz von Microsoft Teams für die Durchführung von freiwilligen Online-Veranstaltungen (z.B. virtuellen Informations- und Vortragsveranstaltungen) sein, wenn der Umfang der Datenverarbeitung sowohl im Hinblick auf die Anzahl der verarbeiteten Daten als auch bezüglich der Kategorien der Betroffenen erheblich beschränkt ist und sich die betroffenen Personen bewusst und freiwillig der Datenverarbeitung unterworfen haben. Auch wenn eine DSFA im Einzelfall nicht notwendig sein sollte, ist es sinnvoll, diese dennoch durchzuführen, um die Rechenschaftspflicht des Verantwortlichen zu erfüllen.

Die Durchführung einer DSFA für den Einsatz von Microsoft 365 durch *[Name der öffentlichen Bildungseinrichtung]* ist *[notwendig / nicht notwendig]*, weil *[Begründung]*.

#### 2.1.4 Prüfgegenstand der DSFA

Hinweis: Prüfgegenstand der DSFA ist der konkrete Einsatz von Microsoft 365 durch die jeweilige öffentliche Bildungseinrichtung und die damit einhergehende Verarbeitung von personenbezogenen Daten. Beide Aspekte bedürfen einer weiteren Erläuterung. Hierzu können insbesondere Informationen zu den folgenden Punkten bereitgestellt werden:

- **Ziel des Einsatzes von Microsoft 365:** Zur Beschreibung des allgemeinen Ziels des Einsatzes von Microsoft 365 können sowohl regulatorische als auch organisatorische Gründe angeführt werden.
- **Vertragsbeziehung mit der Microsoft Ireland Operations Limited:** Die Vertragsbeziehungen mit der Microsoft Ireland Operations Limited (Microsoft Irland)

sollten im Detail beschrieben werden. Insbesondere sollte dargestellt werden, ob und, wenn ja, in welcher Version ein Auftragsverarbeitungsvertrag i.S.d. Art. 28 DSGVO, der sogenannte „Datenschutznachtrag zu den Produkten und Services von Microsoft“ (DPA), vereinbart wurde. Zu berücksichtigen ist, dass Microsoft die Vertragsdokumente von Zeit zu Zeit aktualisiert. So hat Microsoft zuletzt auf die Festlegung der DSK vom 24.11.2022 reagiert und eine aktualisierte Version des [DPA zum 1. Januar 2023](#) veröffentlicht. Verantwortliche sollten die Aktualität ihrer Unterlagen regelmäßig überprüfen und bei Bedarf geeignete Maßnahmen ergreifen.

- **Konkreter Einsatz von Microsoft 365:** Es sollte der konkrete Einsatz von Microsoft 365 durch den Verantwortlichen dargestellt werden. Neben der genutzten Version der Software und ggf. deren Zusammenspiel mit weiteren im Einsatz befindlichen Software-Lösungen sollten insbesondere auch die genutzten (Alternativ-)Anwendungen beschrieben werden. Auch etwaige Ausnahmen oder Besonderheiten bei der Nutzung von Microsoft 365, z.B. Einschränkungen für bestimmte Arten von Daten, sollten dargestellt werden.

#### **2.1.4.1 Beschreibung von Microsoft 365 durch [Name der öffentlichen Bildungseinrichtung]**

Prüfgegenstand der DSFA ist der Einsatz von Microsoft 365 durch [Name der öffentlichen Bildungseinrichtung] und die damit einhergehende Verarbeitung von personenbezogenen Daten, die im Folgenden näher beschrieben werden: [Beschreibung des Prüfgegenstandes]

#### **2.1.4.2 Vertraglicher Rahmen zum Einsatz von Microsoft 365**

Hinweis: Zur Teilnahme am Microsoft-Angebot für öffentliche Bildungseinrichtungen ist der Abschluss bestimmter Verträge erforderlich. Hinzu kommen gegebenenfalls optionale Zusatzvereinbarungen und Informationen von Microsoft. Für den Einsatz von Microsoft 365 an öffentlichen Bildungseinrichtungen sind z.B. die folgenden Vertragsunterlagen zu berücksichtigen:

Vertragliche Grundlagen:

- [Produktbestimmungen](#) (engl. „Product Terms“)
- [Dienstanbieter-Nutzungsrechte](#) (engl. „Services Provider Use Rights“ (SPUR))

- [Vereinbarung zum Servicelevel für Microsoft-Onlinedienste](#) (engl. „Service Level Agreements“ (SLA))
- [Microsoft-Servicevertrag](#) (engl. „Microsoft Services Agreement“)

Nutzung von Microsoft 365 an Bildungseinrichtungen:

- [Hochschulrahmenvertrag](#) mitsamt Zusatzvereinbarungen
- [FWU-Rahmenvertrag](#) mitsamt Zusatzvereinbarungen
- [Beitritt für Bildungslösungen](#) (engl. „Enrollment for Education Solutions“ (EES))
- [Cloud-Solution-Provider-Vertrag](#)
- [Microsoft-Berechtigungskriterien für Qualifizierte Nutzer für Forschung & Lehre \(EMEA\)](#)

Datenschutzrechtliche Dokumente:

- [Datenschutznachtrag zu den Produkten und Services von Microsoft](#) (engl. „Microsoft Products and Services Data Protection Addendum“ (DPA))
- [Microsoft-Datenschutzbestimmungen](#) (engl. „Privacy Statement“)

Die [*Name der öffentlichen Bildungseinrichtung*] hat zum Zwecke des Einsatzes von Microsoft 365 die folgenden Verträge mit Microsoft geschlossen: [*Auflistung der Vertragsdokumente mitsamt deren Bedeutung*]

#### **2.1.4.3 Microsoft 365-Lizenzen der [*Name der öffentlichen Bildungseinrichtung*]**

Hinweis: Das Angebot von Microsoft für öffentliche Bildungseinrichtungen umfasst verschiedene Lizenzmodelle, sog. Microsoft 365 Education-Pläne. Für öffentliche Bildungseinrichtungen gelten die Lizenzmodelle (Education-Pläne) Office 365 A1, Office 365 A3 sowie Office 365 A5.

Zum Zeitpunkt der Erstellung der DSFA bestehen bei der [*Name der öffentlichen Bildungseinrichtung*] die folgenden Lizenzen für Microsoft 365: [*Auflistung der an der öffentlichen Bildungseinrichtung bestehenden Lizenzen*]

#### **2.1.4.4 Von der [*Name der öffentlichen Bildungseinrichtung*] genutzte Anwendungen**

Hinweis: Auch wenn die Lizenzen zahlreiche Anwendungen beinhalten, bedeutet dies nicht, dass die Anwendungen in vollem Umfang tatsächlich genutzt werden. So können

Anwendungen deaktiviert oder deren Einsatz auf organisatorischer Ebene verboten bzw. beschränkt werden. Es sollte daher zur Konkretisierung des Prüfgegenstands eine Darstellung der genutzten bzw. nicht genutzten Anwendungen erfolgen.

An der [Name der öffentlichen Bildungseinrichtung] werden die folgenden Anwendungen der bestehenden Lizenzen genutzt bzw. nicht genutzt: [Auflistung der Anwendungen mit ggf. weiteren Erläuterungen zu deren Einsatz]

### **2.1.5 Verarbeitung personenbezogener Daten**

Hinweis: Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Eine Verarbeitung ist nach Art. 4 Nr. 2 DSGVO jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Beim Einsatz von Microsoft 365 bedient sich die öffentliche Bildungseinrichtung als Verantwortliche (Art. 4 Nr. 7 DSGVO) der Dienste von Microsoft als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO). Hierbei können verschiedene Arten von personenbezogenen Daten von unterschiedlichen Kategorien von Betroffenen verarbeitet werden.

Microsoft verarbeitet zudem losgelöst von der Auftragsverarbeitung Nutzerdaten zu eigenen Zwecken. Diese Datenverarbeitung kann die öffentliche Bildungseinrichtung technisch auf ein Minimum reduzieren. In dem Umfang, in dem Microsoft personenbezogene Daten für eigene Zwecke verarbeitet, stellt Microsoft gemäß den Regelungen des DPA die Einhaltung des Datenschutzrechts sicher.

#### **2.1.5.1 Art der verarbeiteten Daten**

Hinweis: Gemäß dem DPA können je nach Nutzung von Microsoft 365 unterschiedliche

personenbezogene Daten verarbeitet werden. Um die Zulässigkeit der Verarbeitung sowie die damit verbundenen Risiken zu bewerten, empfiehlt es sich, sowohl die verarbeiteten Datenarten sowie beispielhaft erfasste Datentypen anzugeben.

Laut Anhang B des DPA können z.B. die folgenden personenbezogenen Daten verarbeitet werden:

- **Personenbezogene Basisdaten** (z.B. Geburtsort, Straßename und Hausnummer (Adresse), Postleitzahl, Wohnort, Land der Ansässigkeit, Mobiltelefonnummer, Vorname, Nachname, Initialen, E-Mail-Adresse, Geschlecht, Geburtsdatum) einschließlich der personenbezogenen Basisdaten von Familienmitgliedern und Kindern
- **Authentifizierungsdaten** (z.B. Benutzername, Kennwort oder PIN-Code, Sicherheitsfrage, Audit-Protokoll)
- **Kontaktinformationen** (z.B. Adressen, E-Mail-Adressen, Telefonnummern, Social-Media-Kennungen, Notfallkontaktdaten)
- **Eindeutige Identifikationsnummern und Signaturen** (z.B. Sozialversicherungsnummer, Bankkontonummer, Pass- und Ausweisnummer, Führerscheinnummer und Kfz-Zulassungsdaten, IP-Adressen, Personalnummer, Studentennummer, Patientennummer, Signatur, eindeutige Kennung bei Tracking-Cookies oder ähnliche Technologien)
- Pseudonymisierte Kennungen
- Finanz- und Versicherungsinformationen (z.B. Versicherungsnummer, Bankkontoname und -nummer, Kreditkartename und -nummer, Rechnungsnummer, Einkommen, Art der Versicherung, Zahlungsverhalten, Bonität)
- **Geschäftsinformationen** (z.B. Kaufverlauf, Sonderangebote, Abonnementinformationen, Zahlungsverlauf)
- **Biometrische Informationen** (z.B. DNA, Fingerabdrücke und Iris-Erfassungen)
- **Standortdaten** (z.B. Mobilfunk-ID, Geolokalisierungsdaten, Standort bei Beginn/Ende des Anrufs; Standortdaten, die aus der Nutzung von WLAN-Zugriffspunkten abgeleitet werden)
- **Inhaltsdaten** (z.B. Fotos, Videos und Audio)
- **Internetaktivitäten** (z.B. Browserverlauf, Suchverlauf, Lesen, Fernsehen, Radiohören)
- **Geräteidentifikation** (z.B. IMEI-Nummer, SIM-Kartenummer, MAC-Adresse)
- **Profilierung** (z.B. basierend auf beobachteten kriminellen oder antisozialen

Verhaltensweisen oder pseudonymisierten Profilen anhand von aufgerufenen URLs, Click-Streams, Surfprotokolle, IP-Adressen, Domänen, installierten Anwendungen oder Profilen basierend auf Marketingpräferenzen)

- **Personal- und Einstellungsdaten** (z.B. Angabe des Beschäftigungsstatus, Einstellungsinformationen (wie Lebenslauf, Beschäftigungsverlauf, Ausbildungsverlauf), Stellen- und Positionsdaten einschließlich geleisteter Arbeitsstunden, Beurteilungen und Gehalt, Angaben zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Unternehmen)
- **Ausbildungsdaten** (z.B. Ausbildungsverlauf, aktuelle Ausbildung, Noten und Ergebnisse, höchster Abschluss, Lernbehinderung)
- **Staatsbürgerschafts- und Aufenthaltsinformationen** (z.B. Staatsbürgerschaft, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Passdaten, Angaben zum Aufenthaltsort oder zur Arbeitserlaubnis)
- **Informationen**, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt ausgeführt wird
- **Besondere Kategorien von Daten** (z.B. ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit, Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Anklagen)

Bei der Verwendung von Microsoft 365 an der [Name der öffentlichen Bildungseinrichtung] werden die folgenden personenbezogenen Daten verarbeitet: [Auflistung und Beschreibung der Art der verarbeiteten Daten sowie der erfassten Datentypen]

### 2.1.5.2 Kategorien betroffener Personen

Hinweis: Um die Zulässigkeit des Einsatzes von Microsoft 365 sowie die mit dem Einsatz verbundenen Risiken zu bewerten, sollten zudem die Kategorien von Personen, deren personenbezogene Daten verarbeitet werden, aufgelistet werden. Es können z.B. Daten der folgenden Kategorien betroffener Personen verarbeitet werden:

**Beschäftigte der öffentlichen Bildungseinrichtungen:** Hierunter können sämtliche

Mitarbeiter der öffentlichen Bildungseinrichtung unabhängig von ihrem Anstellungsverhältnis gelistet werden, sodass u.a. verbeamtete Mitarbeiter, angestellte Mitarbeiter sowie (externe) Beauftragte unter diese Kategorie fallen können.

**Sonstige interne Nutzer:** Unter sonstigen internen Nutzer sind solche Personen zu verstehen, die der öffentlichen Bildungseinrichtung zugehörig sind, ohne Beschäftigte der öffentlichen Bildungseinrichtung zu sein. Hierunter können z.B. Schülerinnen und Schüler einer Schule oder Studierende einer Universität fallen.

**Externe Nutzer:** Externe Nutzer können alle Personen sein, die weder Beschäftigte noch sonstige interne Nutzer sind, aber zu Zwecken der Kommunikation sowie des Austauschs und/oder der kollaborativen Zusammenarbeit die Anwendungen von Microsoft 365 nutzen.

**Sonstige Dritte:** Die Kategorie der sonstigen Dritten beschreibt solche Personen, die nicht selbst mithilfe der Anwendungen von Microsoft 365 agieren, deren personenbezogene Daten aber innerhalb der Microsoft-365-Infrastruktur durch eine öffentliche Bildungseinrichtung gespeichert oder in sonstiger Art und Weise verarbeitet werden.

Beim Einsatz von Microsoft 365 durch die [*Name der öffentlichen Bildungseinrichtung*] werden personenbezogene Daten der folgenden Kategorien betroffener Personen verarbeitet: [*Auflistung und Beschreibung der Kategorien betroffener Personen sowie der erfassten Personen*]

### 2.1.5.3 Zwecke der Datenverarbeitung

Hinweis: Zuletzt sollten zur Bewertung der Zulässigkeit der Verarbeitung sowie der mit dem Einsatz von Microsoft 365 einhergehenden Risiken die Zwecke der Datenverarbeitung bestimmt werden. Zur Ermittlung der einschlägigen Zwecke für die Nutzung von Microsoft 365 an einer öffentlichen Bildungseinrichtung können z.B. die folgenden Aspekte berücksichtigt werden, nach denen ein Einsatz der Software in Betracht kommen kann:

- zur zeitgemäßen Erfüllung des staatlichen Bildungsauftrags und der diesbezüglichen Wissensvermittlung;
- zur Ermöglichung einer umfassenden Zusammenarbeit und Kommunikation als Hilfsmittel für eine moderne Lehre, Forschung und Verwaltung;
- zur Bereitstellung eines modernen, zeitgemäßen und effizienten Lern-, Lehr- und Arbeitsumfeldes;
- zur Förderung des wissenschaftlichen Diskurses und neuer pädagogischer Ansätze;

- zum Einsatz digitaler Lehr- und Lernsysteme als Hilfsmittel und fester Bestandteil der modernen Erziehungs- und Unterrichtsarbeit;
- zur kollaborativen und standortübergreifenden Zusammenarbeit;
- zur Vor- und Nachbereitung sowie der Dokumentation der Lehrveranstaltungen;
- zur Vereinfachung des Erstellens und Bearbeitens von Dokumenten und Inhalten;
- zur Bereitstellung und zum Austausch von Dokumenten und anderen Dateien;
- zur Erleichterung und Verbesserung der internen und externen Kommunikation.

Neben der Nennung der einschlägigen Zwecke im Allgemeinen können die verantwortlichen Stellen die Zwecke präzisieren und im Rahmen der Beschreibung der einzelnen Nutzungsszenarien die konkreten Zwecke für die jeweiligen Verarbeitungsvorgänge im Detail weiter erläutern.

Die Zwecke der [Name der öffentlichen Bildungseinrichtung] für den Einsatz von Microsoft 365 sind: [Auflistung aller Zwecke].

### **2.1.6 Beschreibung der Nutzungsszenarien**

Hinweis: Die Anwendungen von Microsoft 365 sind vielseitig einsetzbar. Um eine Grundlage für die datenschutzrechtliche Bewertung festzulegen, ist eine Eingrenzung der Nutzung der Anwendungen erforderlich. Hierzu können die verschiedenen Einsatzbereiche der Anwendungen (Nutzungsszenarien) an einer öffentlichen Bildungseinrichtung festgelegt werden. Die Festlegung der Nutzungsszenarien kann auf unterschiedliche Art und Weise erfolgen. Zur Strukturierung der Verarbeitungsvorgänge können z.B. die Anwendungen in ihre jeweiligen Aufgabengebiete eingeteilt werden. So können z.B. die folgenden Nutzungsszenarien gebildet werden:

- Nutzung von Microsoft 365 zur Erstellung und Bearbeitung von Inhalten (z.B. Office-Anwendungen);
- Nutzung von Microsoft 365 zur Kommunikation via E-Mail und zur Kalenderverwaltung (z.B. Microsoft Outlook, Exchange Online);
- Nutzung von Microsoft 365 zur kollaborativen Zusammenarbeit (z.B. Microsoft Teams, Microsoft 365 Groups);
- Nutzung von Microsoft 365 zur Ablage von Dateien und Inhalten (z.B. Microsoft

OneDrive, Microsoft Stream).

Innerhalb der identifizierten Nutzungsszenarien können die relevanten Anwendungen und die Verarbeitungsvorgänge herausgefiltert werden. Anhand dieser Eingrenzung können die betroffenen Personengruppen und die betroffenen Datenkategorien und Datentypen bestimmt werden. Als mögliche Kategorien der Betroffenen sowie als mögliche verarbeitete Datenkategorien und erfasste Datentypen kommen die zuvor genannten Kategorien in Betracht, die es für jedes Nutzungsszenario zu bestimmen gilt. Zuletzt können die einzelnen Zwecke für die jeweiligen Nutzungsszenarien der relevanten Anwendungen evaluiert werden, wobei die zuvor genannten Zwecke für die einzelnen Nutzungsszenarien präzisiert werden sollten. Die Bewertung der datenschutzrechtlichen Zulässigkeit des Einsatzes von Microsoft 365 erfolgt sodann auf Basis der festgelegten Einsatzbereiche und der damit verbundenen Verarbeitungsvorgänge.

Für die *[Name der öffentlichen Bildungseinrichtung]* lassen sich die folgenden Nutzungsszenarien für Microsoft 365 identifizieren: *[Beschreibung der einzelnen Nutzungsszenarien]*

Hinweis: Zur Beschreibung der einzelnen Nutzungsszenarien empfehlen wir, pro Nutzungsszenario die folgenden Punkte aufzunehmen:

- Allgemeine Beschreibung des Nutzungsszenarios
- Beschreibung der für das Nutzungsszenario eingesetzten Anwendungen
- Beschreibung der Art der verarbeiteten Daten, der Betroffenenkategorien und der Verarbeitungszwecke bezogen auf das konkrete Verarbeitungsszenario

### **2.1.7 Verantwortliche für die Verarbeitung**

Hinweis: Wird an einer öffentlichen Bildungseinrichtung Microsoft 365 eingesetzt, so entscheidet in der Regel die Leitung der öffentlichen Bildungseinrichtung über die Zwecke und Mittel der mit dem Einsatz der Software verbundenen Verarbeitung personenbezogener Daten und ist damit Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO. Die Leitung der öffentlichen Bildungseinrichtung bedient sich der Dienste von Microsoft Irland, die im Auftrag der öffentlichen Bildungseinrichtung die Verarbeitungsvorgänge ausführt und als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO tätig wird.

### 2.1.7.1 Verantwortlichkeit der *[Name der öffentlichen Bildungseinrichtung]*

Hinweis: Es sollte an dieser Stelle näher erläutert werden, bezüglich welcher Verarbeitungsvorgänge die öffentliche Bildungseinrichtung als Verantwortliche agiert und welche vertraglichen Regelungen für das Auftragsverarbeitungsverhältnis mit Microsoft Irland gelten. Hierbei sollte insbesondere auf die Notwendigkeit des Abschlusses eines Auftragsverarbeitungsvertrages mit Microsoft Irland eingegangen werden. Diesbezüglich ist zu berücksichtigen, dass Microsoft eine aktualisierte Version seines DPA zum 1. Januar 2023 veröffentlicht hat, das wesentliche Änderungen enthält, die eine Reaktion auf die Kritik der Datenschutzaufsichtsbehörden vom 24.11.2022 darstellen.

[Beschreibung der Verantwortlichkeit der öffentlichen Bildungseinrichtung]

Hinweis: Neben der Darstellung des Auftragsverarbeitungsverhältnisses mit Microsoft sollten auch Vertragsbeziehungen mit sonstigen Auftragsverarbeitern, die bei der Nutzung von Microsoft 365 unterstützen, oder Drittanbieter von Anwendungen, die in Microsoft 365 integriert werden, beschrieben werden. Neben der Nennung des Auftragsverarbeiters sollten dessen Funktion sowie die einschlägigen Vertragsdokumente, insbesondere der Auftragsverarbeitungsvertrag, aufgenommen werden.

### 2.1.7.2 Microsoft Ireland Operations Limited

Hinweis: Neben der Datenverarbeitung im Auftrag des Kunden behält sich Microsoft in dem DPA vor, selbst bestimmte Nutzerdaten zu eigenen Zwecken zu verarbeiten. Microsoft gibt an, statistische, nichtpersonenbezogene Daten aus pseudonymisierten Daten zu aggregieren und Statistiken zu erstellen. Microsoft sichert dabei zu, weder auf die Inhalte von Kundendaten zuzugreifen noch diese zu analysieren. Die Verarbeitungszwecke werden in dem DPA abschließend festgelegt und bestehen in der Abrechnungs- und Kontoverwaltung, der Vergütung wie etwa Berechnung von Mitarbeiterprovisionen und Partner-Incentives, der internen Berichterstattung und Geschäftsmodellierung wie etwa Prognose, Umsatz, Kapazitätsplanung und Produktstrategie und der Finanzberichterstattung. Darüber hinaus sichert Microsoft vertraglich zu, dass Microsoft bei den genannten Verarbeitungsvorgängen die Grundsätze der Datenminimierung anwendet und keine Kundendaten, Professional-Services-Daten oder personenbezogene Daten für die Zwecke der Benutzerprofilerstellung, Werbung

oder ähnliche kommerzielle Zwecke oder sonstige Zwecke verwendet oder verarbeitet. Diese Datenverarbeitung kann auf ein Minimum reduziert werden. In dem Umfang, in dem Microsoft personenbezogene Daten für seine eigenen Geschäftszwecke verarbeitet, ist Microsoft gemäß dem DPA selbst für die Einhaltung aller geltenden Datenschutzbestimmungen verantwortlich.

[Kurze Beschreibung der Verantwortlichkeit von Microsoft Irland]

### 2.1.8 Rechtsgrundlagen

Hinweis: Die DSGVO enthält den Grundsatz des Verbots mit Erlaubnisvorbehalt. Hiernach darf eine Verarbeitung personenbezogener Daten nur erfolgen, wenn ein gesetzlicher Erlaubnistatbestand erfüllt ist. Die Erlaubnistatbestände ergeben sich in erster Linie aus Art. 6 DSGVO sowie den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) und des anwendbaren Landesdatenschutzgesetzes (LDSG). Zur Bestimmung der einschlägigen Rechtsgrundlagen ist zwischen den Datenverarbeitungsprozessen zu unterscheiden. So können Rechtsgrundlagen für alle Nutzungsszenarien bezüglich des Einsatzes von Microsoft 365 vorliegen oder aber spezifische Rechtsgrundlagen für bestimmte Personengruppen oder bestimmte Verarbeitungsvorgänge einschlägig sein. Die Rechtsgrundlagen können kumulativ herangezogen werden. Beim Einsatz von Microsoft 365 durch eine öffentliche Bildungseinrichtung erscheinen insbesondere die folgenden Rechtsgrundlagen denkbar:

- **Erfüllung einer Aufgabe im öffentlichen Interesse:** Für die Verarbeitung der personenbezogenen Daten aller betroffenen Personen bezüglich sämtlicher Nutzungsszenarien einer öffentlichen Bildungseinrichtung könnte zunächst Art. 6 Abs. 1 S. 1 lit. e) Alt. 1 DSGVO in Betracht kommen. Hiernach ist eine Verarbeitung rechtmäßig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt und der verantwortlichen Stelle übertragen wurde. Daneben können auch die entsprechenden Regelungen des einschlägigen LDSG angeführt werden. Im Rahmen der weiteren Prüfung könnte berücksichtigt werden, dass die öffentliche Bildungseinrichtung nach dem jeweiligen Landesrecht ausdrücklich zur Erfüllung ihres Auftrags digitale Lehr- und Lernsysteme einsetzen kann. Zuletzt ist die Erforderlichkeit der Verarbeitung für die Aufgabenerfüllung darzulegen, wobei die Interessen der Beteiligten abzuwägen sind und die Eingriffe in die Rechte der Betroffenen auf das Notwendigste beschränkt werden

sollten.

- **Ausübung öffentlicher Gewalt:** Für einzelne Aufgaben könnte die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. e) Alt. 2 DSGVO in Betracht kommen. Hiernach ist eine Verarbeitung dann zulässig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die in Ausübung öffentlicher Gewalt erfolgt, die der verantwortlichen Stelle übertragen wurde. Auch hier könnte daneben die Vorschrift des jeweiligen LDSG genannt werden, sofern diese eine gleichlautende Regelung enthält. Unter der Ausübung öffentlicher Gewalt ist die Wahrnehmung hoheitlicher Aufgaben auf der Grundlage rechtlich festgelegter Aufgaben und Befugnisse zu verstehen.<sup>3</sup> Hier könnte z.B. berücksichtigt werden, dass der öffentlichen Bildungseinrichtung durch das jeweilige Landesrecht öffentliche Gewalt zur Erfüllung ihrer Aufgaben übertragen wird. Darüber hinaus bedarf es der Darlegung der hoheitlichen Aufgaben, zu deren Erfüllung Microsoft 365 im Einzelfall eingesetzt wird. Ein Beispiel hierfür könnte die Durchführung von Prüfungen sein, sofern es sich z.B. im Rahmen der Benotung und der Bewertung um einen hoheitlichen Akt, einen Verwaltungsakt i.S.v. § 35 VwVfG handelt,<sup>4</sup> was ebenfalls für den Einzelfall erläutert werden sollte. Zuletzt bedarf es auch hier einer umfassenden Interessenabwägung zur Begründung der Erforderlichkeit der Verarbeitung zur Erfüllung der zuvor genannten Aufgabe, die in Ausübung öffentlicher Gewalt erfolgt.
- **Nicht verbeamtete Beschäftigte:** Für die Verarbeitung von personenbezogenen Daten von nicht verbeamteten Beschäftigten können unterschiedliche Rechtsgrundlagen in Betracht kommen: Für die Verarbeitung personenbezogener Daten von nicht verbeamteten Beschäftigten könnte im Falle einer Lehrtätigkeit die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. b), Art. 88 Abs. 1 DSGVO i.V.m. § 26 BDSG einschlägig sein. Hiernach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer

---

<sup>3</sup> Siehe *Heberlein* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 22.

<sup>4</sup> Siehe *von Alemann/Scheffczyk* in: Bader/Ronellenfisch, BeckOK VwVfG, 57. Ed., Stand: 01.10.2022, § 35 VwVfG, Rn. 180.

Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Für die Verarbeitung personenbezogener Daten von nicht verbeamteten Beschäftigten im Bereich der Verwaltungstätigkeiten könnte Art. 6 Abs. 1 S. 1 lit. b), Art. 88 Abs. 1 DSGVO i.V.m. der jeweiligen Vorschrift des LDSG Anwendung finden. Bezüglich der Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO könnte entsprechend der obigen Unterscheidung die Rechtsgrundlage zum einen auf Art. 6 Abs. 1 S. 1 lit. b), Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 3 BDSG bzw. zum anderen auf Art. 6 Abs. 1 S. 1 lit. b), Art. 88 Abs. 1 DSGVO i.V.m. der Regelung des jeweiligen LDSG gestützt werden. Danach kann eine Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses bzw. für Zwecke des Dienst- und Beschäftigungsverhältnisses zulässig sein, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Zuletzt könnte für bestimmte Einzelfälle des Einsatzes von Microsoft 365 auch die Rechtsgrundlage nach Art. 6 Abs. 1 S. 1 lit. b), Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG in Betracht kommen. Hiernach dürfen zur Aufdeckung von Straftaten personenbezogene Daten von Beschäftigten verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

- **Verbeamtete Beschäftigte:** Für die Verarbeitung personenbezogener Daten von verbeamteten Beschäftigten könnte insbesondere die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. c) DSGVO in Betracht kommen. Hiernach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der die verantwortliche Stelle unterliegt. Im Rahmen der Prüfung dieser Rechtsgrundlage könnte die öffentliche Bildungseinrichtung z.B. die Regelungen des Landesrechts berücksichtigen, welche die (Dienst-)Aufgaben der

öffentlichen Bildungseinrichtung und ihrer Beschäftigten regeln. Auch könnte berücksichtigt werden, dass sich eine rechtliche Verpflichtung auch aus Art. 33 Abs. 5 Grundgesetz (GG) ergeben könnte. So ist das Recht des öffentlichen Dienstes unter Berücksichtigung der hergebrachten Grundsätze des Berufsbeamtentums zu regeln und fortzuentwickeln.

- **Einwilligung:** Sofern es die Umstände des Einzelfalls zulassen, könnte eine Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO i.V.m. der konkreten Einwilligungserklärung des Betroffenen als Rechtsgrundlage in Betracht kommen. Erforderlich hierfür ist, dass die erteilte Einwilligung freiwillig und informiert erfolgt. Diese Voraussetzungen sind für den Einzelfall darzulegen. Hierbei sollte insbesondere im Verhältnis öffentliche Bildungseinrichtung – Lernende begründet werden, weshalb trotz des Über-unter-Verhältnisses eine freiwillige Erklärung durch die Betroffenen erfolgen kann. Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, könnte eine Einwilligung nach Art. 9 Abs. 2 lit. a) DSGVO in Betracht kommen. Voraussetzung hierfür ist, dass die Einwilligung nicht nur den allgemeinen Anforderungen entspricht, sondern auch die besonderen Anforderungen des Art. 9 Abs. 2 lit. a) DSGVO erfüllt, wonach insbesondere eine ausdrückliche Einwilligung der Betroffenen erforderlich ist.
- **Vertragserfüllung:** Eine Datenverarbeitung könnte im Einzelfall auch auf den Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 lit. b) DSGVO gestützt werden. Hiernach ist eine Verarbeitung rechtlich zulässig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen. Diese Rechtsgrundlage könnte z.B. für bestimmte Fälle des Einsatzes von Microsoft 365 in der Kommunikation mit externen Dritten in Betracht kommen. Entscheidend ist hierbei jeweils, dass zwischen der verantwortlichen Stelle und den Betroffenen nicht nur eine (vor)vertragliche Beziehung besteht, sondern der konkrete Verarbeitungsvorgang auch erforderlich sein muss.
- **Rechtsgrundlage für die Offenlegung von Daten an Microsoft:** Ob durch den bloßen Einsatz von Microsoft 365 neben der inhaltlichen Datenverarbeitung auch ein eigenständiger Verarbeitungsvorgang im Sinne einer Offenlegung der Daten an Microsoft, die Microsoft zu eigenen Zwecken verarbeitet, vorliegt, ist umstritten. Folgt man der [Ansicht der DSK](#) und bejaht eine Offenlegung, ist auch hierfür eine

Rechtsgrundlage erforderlich. Der DSK ist insoweit zuzustimmen, dass den öffentlichen Bildungseinrichtungen aufgrund der Regelung des Art. 6 Abs. 1 S. 2 DSGVO ein unmittelbarer Rückgriff auf die Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO in der Regel verwehrt bleibt. Jedoch bildet Art. 6 Abs. 1 S. 1 lit. f) DSGVO nicht die einzige Möglichkeit, eine datenschutzkonforme Offenlegung der Daten gegenüber Microsoft zu begründen. Stattdessen kann die Vorschrift des § 25 Abs. 2 BDSG oder der jeweiligen LDSG einschlägig sein. Auch kann das Landesrecht spezifische Rechtsgrundlagen hierzu enthalten. Nach diesen Normen kann eine Übermittlung personenbezogener Daten an nicht öffentliche Stellen zulässig sein, wenn der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt, – je nach Vorschrift – die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Diese Voraussetzungen können im Hinblick auf die strengen vertraglichen Regelungen des DPA von Microsoft erfüllt sein. Es ist jedoch zu berücksichtigen, dass die genannten Vorschriften teilweise für europarechtswidrig gehalten werden. Es bedarf daher einer eingehenden Prüfung im Einzelfall.

Die jeweilige Bildungseinrichtung sollte die genannten Rechtsgrundlagen prüfen und, sofern sie sich auf eine oder mehrere der Erlaubnistatbestände berufen möchte, ihre Prüfung in dokumentierter Weise im Folgenden hinreichend darlegen.

Die [Name der öffentlichen Bildungseinrichtung] stützt sich im vorliegenden Fall mit der folgenden Begründung auf die folgenden Rechtsgrundlagen: [Beschreibung der Rechtsgrundlagen mitsamt der Begründung des Vorliegens der jeweiligen Tatbestandsvoraussetzungen]

### **2.1.9 Drittlandsübermittlung**

Hinweis: Bei einem Einsatz von Microsoft 365 kann eine Übermittlung von personenbezogenen Daten in ein Drittland, also ein Land, das weder Mitglied der EU noch des Europäischen Wirtschaftsraums (EWR) ist, nicht ausgeschlossen werden. Nach [Angaben von Microsoft](#) werden zwar Daten, die aus der Globalen Region 1 (EMEA) stammen, grundsätzlich an

Standorten innerhalb der EU verarbeitet. Hierbei handelt es sich jedoch ausdrücklich nur um die Speicherung der ruhenden Kundendaten („data at rest“). Daten in der Übermittlung („in transit“) können über andere Standorte geleitet und in anderen Regionen verarbeitet werden. In [weiteren Informationen](#) zu den Datenspeicherorten für die EU erklärt Microsoft zudem, dass trotz der Standortregelung eine vorübergehende Datenübertragung außerhalb der genannten geografischen Grenze erforderlich sein kann.

Die DSGVO stellt hohe Anforderungen an Drittlandsübermittlungen (Art. 44 ff. DSGVO). Eine Drittlandsübermittlung ist nur möglich, wenn ein Angemessenheitsbeschluss der Europäischen Kommission (EU-Kommission) vorliegt, der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien zum Schutz der personenbezogenen Daten vorgesehen hat oder eine der Ausnahmen des Art. 49 DSGVO greift. Die Vorschriften sind primär von dem Datenexporteur, also der Person, die die Daten an einen Empfänger in einem Drittland übermittelt, zu beachten. Datenexporteur kann sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter sein.

Ein Schwerpunkt der [Kritik der DSK](#) am Einsatz von Microsoft 365 lag bisher auf der Datenübermittlung in das Drittland USA. Nach Ansicht der Datenschutzaufsichtsbehörden konnten die Voraussetzungen der [„Schrems II“-Entscheidung](#) des Europäischen Gerichtshofs (EuGH) in den meisten Fällen nicht oder nur sehr schwer eingehalten werden. Andere Stimmen vertreten, dass zumindest im konkreten Einzelfall unter Berücksichtigung aller Umstände und insbesondere der ergriffenen Schutzmaßnahmen die Anforderungen der DSGVO auch bei dem Einsatz von Microsoft 365 erfüllt werden können. Zu diesem Zweck hat Microsoft vielfältige Maßnahmen ergriffen und entsprechende Informationen zur Verfügung gestellt. Ausgehend davon ist es erforderlich, dass die öffentlichen Bildungseinrichtungen eine eigene Bewertung der rechtlichen Zulässigkeit der Drittlandsübermittlungen vornehmen und diese in dokumentierter Weise begründen.

Im Rahmen dieser Bewertung können entsprechend den Erklärungen und Informationen von Microsoft insbesondere die folgenden Aspekte berücksichtigt werden: Beim Einsatz von Microsoft 365 übermittelt Microsoft Irland als Datenexporteur personenbezogene Daten an Microsoft Corporation als Datenimporteur mit Sitz in den USA. Zu diesem Zweck hat Microsoft Irland die aktuellen Standardvertragsklauseln (Standard Contractual Clauses (SCC)) der EU-Kommission in dem Modul drei „Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter“

abgeschlossen und veröffentlicht. Im Verhältnis zu seinen Kunden verpflichtet sich Microsoft Irland in dem DPA von Januar 2023 zudem vertraglich, die aktuellen SCC der EU-Kommission mit der Microsoft Corporation abzuschließen und ein sog. „Transfer Impact Assessment“ durchzuführen. Eine Offenlegung von Daten erfolgt nur nach dem Maßstab des EU-Rechts (Art. 23 DSGVO). Verantwortliche, die Microsoft 365 einsetzen, sollten daher sicherstellen, dass sie das aktuelle DPA mit Microsoft vereinbart haben. Microsoft stellt darüber hinaus weitere Informationen zu Drittlandsübermittlungen in die USA und Erklärungen zur Verfügung, die nach der „Schrems II“-Entscheidung ebenfalls zu berücksichtigen sind.

Im Hinblick auf künftige Entwicklungen zu Datenübermittlungen in die USA kann zudem berücksichtigt werden, dass sich die EU und die USA auf ein gemeinsames Datenschutzabkommen, das sog. „Trans-Atlantic Data Privacy Framework“ oder auch „EU-U.S. Data Privacy Framework“,  geeinigt haben und die USA ihre Selbstverpflichtungen hieraus bereits in einem Rechtsakt, der sogenannten „Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities“ (EO), umgesetzt haben. Die EU-Kommission hat in der Folge bereits einen Entwurf für einen neuen Angemessenheitsbeschluss veröffentlicht und das Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA eingeleitet. Der Erlass des neuen Angemessenheitsbeschlusses wird für Mitte des Jahres erwartet. Auch Microsoft selbst hat mit dem „EU Data Boundary for the Microsoft Cloud“ (EU Data Boundary) (auf Deutsch „EU-Datengrenze für die Microsoft Cloud“) eine neue – europäische – Lösung für die Verarbeitung von Daten von Kunden aus der EU angekündigt und bereits im Januar 2023 mit der schrittweisen Umsetzung begonnen. Die aktuellen Entwicklungen sollten fortlaufend beobachtet und bei Bedarf geeignete Maßnahmen durch die öffentliche Bildungseinrichtung ergriffen werden.

[Darlegung der Drittlandsübermittlungen bei Microsoft 365 sowie deren rechtliche Zulässigkeit]

### **2.1.10 Gewährleistung der Betroffenenrechte**

Hinweis: Ein wichtiges Ziel der DSGVO ist der Schutz von Betroffenen. Ihnen stehen eine Reihe von Rechten gemäß des Kapitels 3 der DSGVO zur Verfügung (z.B. Recht auf Information, Art. 12 ff. DSGVO, Recht auf Auskunft, Art. 15 DSGVO oder Recht auf Löschung, Art. 17 DSGVO). Die Gewährleistung dieser Rechte hat die öffentliche Bildungseinrichtung sicherzustellen und

hierfür geeignete Maßnahmen zu ergreifen. Hierzu können insbesondere die folgenden Maßnahmen berücksichtigt werden:

- Bereitstellung von Informationen über die Verarbeitung für die Betroffenen (z.B. mithilfe von Rundschreiben);
- Dokumentation von Einwilligungen der Betroffenen, sofern ein Verarbeitungsvorgang auf die Rechtsgrundlage der Einwilligung gestützt wird;
- Prozesse zur Bearbeitung von Betroffenenanfragen (z.B. mithilfe des sogenannten [„DSR \(Data Subject Request\) Case Tool“](#) (auf Deutsch „UDS-Falltool“) von Microsoft);
- Ermöglichung der Meldung von Verhaltensverstößen an eine Meldestelle der öffentlichen Bildungseinrichtung.

Bezüglich der Information der Betroffenen ist zudem zu beachten, dass auch Microsoft zahlreiche Informationen für Verantwortliche und Betroffene bereitstellt. In dem News Center von Microsoft gibt es z.B. eine [eigene Rubrik zum Datenschutz](#). Als relevante Beiträge sind hierbei u.a. die Beiträge der Reihe [„Faktencheck Datenschutz“](#) sowie die Reihe [„Im Daten-Dschungel“](#) hervorzuheben.

Wir empfehlen sämtliche Maßnahmen, die die Gewährleistung der Betroffenenrechte sicherstellen, im Folgenden aufzunehmen.

[Darstellung der konkreten Gewährleistung der Betroffenenrechte im Einzelfall]

### 2.1.11 Löschung der Daten

Hinweis: Nach den Datenschutzgrundsätzen der Datenminimierung (Art 5 Abs. 1 lit. c) DSGVO) und der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO) dürfen personenbezogene Daten nur in einem solchen Umfang und nur für einen solchen Zeitraum verarbeitet werden, wie es für die Verarbeitungszwecke erforderlich ist. Personenbezogene Daten, die nicht mehr für die jeweiligen Verarbeitungszwecke benötigt werden, sind zu löschen. Wir empfehlen ein Löschkonzept für den Einsatz von Microsoft 365 zu erstellen und auf dieses Bezug zu nehmen. Neben der Darstellung des eigenen Löschkonzepts können auch die [Informationen von Microsoft zur Löschung von Daten](#) aufgenommen werden.

[Beschreibung des Löschkonzepts der öffentlichen Bildungseinrichtung]

## 2.2 Notwendigkeit und Verhältnismäßigkeit der Verarbeitung (Art. 35 Abs. 7 lit. b) DSGVO)

Hinweis: Nach Art. 35 Abs. 7 lit. b) DSGVO hat eine DSFA eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck zu beinhalten. Bezugspunkt der Verhältnismäßigkeit der Datenverarbeitung ist Art. 5 Abs. 1 lit. b) und lit. c) DSGVO, der die Grundsätze der Zweckbindung und der Datenminimierung enthält. Die Datenverarbeitung muss nicht nur auf einer Rechtsgrundlage beruhen, sondern auch verhältnismäßig sein. Die Prüfung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung unterteilt sich hierbei in die folgenden Punkte:

- Vorliegen eines legitimen Zwecks;
- Geeignetheit der Verarbeitung;
- Notwendigkeit der Verarbeitung;
- Angemessenheit der Verarbeitung.

Ein **legitimer Zweck** kann grundsätzlich in jedem berechtigten Zweck liegen, der nicht in Widerspruch zu Recht und Gesetz steht. Da die Bildungseinrichtungen als öffentliche Stellen agieren, muss der legitime Zweck in einem öffentlichen Interesse liegen. Für den Einsatz von Microsoft 365 an öffentlichen Bildungseinrichtungen könnten z.B. die folgenden Zwecke in Betracht kommen:

- Ermöglichung und Verbesserung eines digitalen Arbeitsumfelds;
- Etablierung digitaler Arbeitsabläufe und Ermöglichung effektiver Arbeitsstrukturen;
- Verbesserung und Erleichterung der Kommunikations- und Arbeitsstrukturen sowohl intern als auch nach außen;
- Stärkung der Attraktivität der öffentlichen Bildungseinrichtung;
- Etablierung einer effizienten unterrichtlichen Organisationstätigkeit der öffentlichen Bildungseinrichtung.

Darüber hinaus muss die mit dem Einsatz von Microsoft 365 einhergehende Datenverarbeitung im Hinblick auf den Zweck **geeignet** sein. Eine Verarbeitung personenbezogener Daten ist dann geeignet, wenn sie den legitimen Zweck objektiv fördert.

Der Einsatz von Microsoft 365 muss zudem für das Erreichen der legitimen Zwecke **erforderlich** sein. Dies ist zu bejahen, wenn die legitimen Zwecke nicht mit anderen, gleich geeigneten, aber weniger eingreifenden Mittel erreicht werden können. Eine Datenverarbeitung ist erforderlich, wenn die Zielerreichung im konkreten Einzelfall ohne die Verarbeitung nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfolgen kann. Die Datenverarbeitung muss sich auf das Notwendige beschränken. Sollten alternative, gleich geeignete mildere Mittel zur Verfügung stehen, muss die verantwortliche Stelle zwingend auf diese Alternativen zurückgreifen. Ein Mittel zählt als milder, wenn es Betroffene weniger stark in ihren Rechten einschränkt.<sup>5</sup> Der Einsatz der alternativen Mittel muss für den Verantwortlichen jedoch objektiv zumutbar sein.<sup>6</sup> Es kann nichts rechtlich oder tatsächlich Unmögliches verlangt werden. Die Unzumutbarkeit alternativer Maßnahmen bestimmt sich anhand einer Interessenabwägung. Entscheidende Bedeutung wird hierbei der finanziellen und personellen Realisierbarkeit der Maßnahmen zukommen.<sup>7</sup> Zur Begründung der Erforderlichkeit des Einsatzes von Microsoft 365 können z.B. die folgenden Aspekte erörtert werden:

- Erfüllung des staatlichen Bildungsauftrags im digitalen Zeitalter;
- Etablierung als zukunftsweisende Bildungseinrichtung mit entsprechenden Angeboten;
- Aufrechterhaltung des allgemeinen Lehr- und Verwaltungsbetriebs in Zeiten der Corona-Pandemie;
- Erfüllung der Erwartungen an eine zeitgemäße und moderne Bildungseinrichtung;
- Anpassung an geänderte gesetzliche und gesellschaftliche Rahmenbedingungen;
- Gewährleistung effizienter Prozesse nach dem aktuellen Stand der Technik;
- Vertrautheit der Nutzer mit Microsoft 365.

Zuletzt muss der Einsatz von Microsoft 365 und der einhergehenden Datenverarbeitung **angemessen** sein. Eine Datenverarbeitung ist angemessen, wenn die Interessenabwägung im Rahmen einer Zweck-Mittel-Relation zugunsten des Verantwortlichen ausfällt. Die Interessen der Betroffenen sind mit den Interessen des Verantwortlichen abzuwägen. Es sind zunächst die Interessen des Verantwortlichen und der Betroffenen herauszuarbeiten und diese sodann in ein angemessenes Verhältnis zu bringen. Es sollte eine Auseinandersetzung mit den Interessen,

---

<sup>5</sup> Siehe *Wolff* in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, D. Grundprinzipien und Zulässigkeit der Datenverarbeitung, Rn. 434.

<sup>6</sup> Siehe *Schulz* in: Gola/Heckmann, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 38.

<sup>7</sup> Siehe *Wolff* in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed., Stand: 01.11.2021, § 3 BDSG Rn.17.

Grundrechten und Grundfreiheiten der Beteiligten bezogen auf den konkreten Einzelfall erfolgen. Hierbei können z.B. die folgenden Aspekte berücksichtigt werden:

- Schutz der Privatsphäre während der Lern-, Lehr- und Arbeitszeit;
- Anforderungen und Erwartungen der betroffenen Personen im heutigen digitalen Zeitalter;
- Vorteile des Einsatzes von Microsoft 365 für die Betroffenen;
- Maßnahmen der verantwortlichen Stellen zur Eindämmung der Datenschutzrisiken;
- Einsatz von Microsoft 365 nur nach der tatsächlichen Erforderlichkeit sowie ausdifferenzierte Auswahl beim Einsatz von Software;
- Bereitstellung von alternativen, äquivalenten Angeboten.

[Beschreibung der Verhältnismäßigkeitsprüfung]

### **2.3 Risikoanalyse (Art. 35 Abs. 7 lit. c) DSGVO)**

Hinweis: Nach Art. 35 Abs. 7 lit. c) DSGVO ist im Rahmen einer DSFA eine Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen durchzuführen.

Zur Ermittlung der Risiken bedarf es einer zuvor festgelegten Methodik. Das Risiko für die Betroffenen ergibt sich aus einer Zusammenschau der Eintrittswahrscheinlichkeit einer Bedrohung und dem mit der Bedrohung verbundenen potenziellen Schaden. Ob ein Risiko vorliegt und wenn ja, wie das Risiko zu gewichten ist, ist aus der Sicht der Betroffenen zu bewerten. Um das konkrete Einzelrisiko bestimmen zu können, hat sich die Risikobewertung anhand einer Risikomatrix bewährt:

Schaden	groß	4	8	12	16
	substanziell	3	6	9	12
	überschaubar	2	4	6	8
	gering	1	2	3	4
	X	gering	überschaubar	substanziell	groß
<b>Eintrittswahrscheinlichkeit</b>					

Die Risikomatrix dient dazu, die Datensicherheitsziele (Verfügbarkeit, Integrität, Vertraulichkeit) sowie die Datenschutzziele (Verfügbarkeit, Integrität, Vertraulichkeit, Zweckbindung, Datenminimierung, Transparenz und Nichtverkettbarkeit) zu bewerten. Die einzelnen Risiken werden basierend auf der Wahrscheinlichkeit des Eintritts und der Schwere der Folgen des Risikoeintritts (Schaden) in die Kategorien „gering“, „überschaubar“, „substanziell“ und „groß“ eingeteilt. Die Eintrittswahrscheinlichkeit ist hierbei ein Schätzwert für das Eintreten eines Risikos. Der potenzielle Schaden der Betroffenen wird anhand der genannten Schutzziele der DSGVO geschätzt. Hierzu wird geprüft, inwiefern bestimmte Ereignisse zum Eintritt eines physischen, materiellen oder immateriellen Schadens für die Betroffenen (siehe Erwägungsgrund 75 DSGVO) führen können.

Nach der Ermittlung der Eintrittswahrscheinlichkeit sowie der Schwere des Schadens ist der Wert der Eintrittswahrscheinlichkeit mit dem Wert des Schadens zu multiplizieren. Mithilfe des ermittelten Wertes wird sodann in der Risikomatrix eine Risikoklasse festgelegt, wobei der höchste Schadenswert zugrunde gelegt wird.

Die Risikobewertung bezieht sich zunächst auf die Ermittlung des Brutto Risikos, sodass in dem folgenden Abschnitt zunächst für die jeweiligen Verarbeitungsvorgänge Risikoszenarien gebildet werden und diese zunächst ohne Abhilfemaßnahmen begutachtet werden sollten. Erst

im Abschnitt der Ermittlung und Bewertung von Abhilfemaßnahmen können alle relevanten Abhilfemaßnahmen dargestellt und deren Auswirkungen auf die ermittelten Risiken erläutert werden. Zuletzt sollte eine abschließende Bewertung der Risiken unter Einbeziehung der implementierten Abhilfemaßnahmen erfolgen.

### **2.3.1 Risiken bei Einsatz von Microsoft 365 an der [Name der öffentlichen Bildungseinrichtung]**

Hinweis: Die konkreten Risiken sind individuell für den Einzelfall des Einsatzes von Microsoft 365 bei der verantwortlichen Stelle zu identifizieren. Allerdings verweisen mehrere Datenschutzaufsichtsbehörden der Länder auf potenzielle Risiken beim Einsatz von Microsoft 365 an Bildungseinrichtungen, die in jedem Fall im Rahmen der Risikoanalyse berücksichtigt werden sollten.<sup>8</sup> Darüber hinaus haben sich allgemein bestimmte potenzielle Risiken beim Einsatz von Microsoft 365 in der Vergangenheit herauskristallisiert. Ausgehend davon können z.B. die folgenden Risiken beim Einsatz von Microsoft 365 an öffentlichen Bildungseinrichtungen in Betracht kommen:

- unzulässiger Zugriff auf personenbezogene Daten durch US-Behörden;
- unbefugte (Weiter-)Verarbeitung von Daten durch Microsoft zu eigenen Zwecken;
- Überwachung des Nutzerverhaltens durch Microsoft durch die Verarbeitung von Metadaten;
- Verwendung der Daten für Werbezwecke;
- Intransparenz der Datenverarbeitungsprozesse;
- Kenntnisnahme von Daten durch Microsoft;
- Eintritt eines Überwachungseffektes für Nutzer;
- unbefugte Weitergabe von Daten durch einen Nutzer von Microsoft 365;
- (unbeabsichtigte) Löschung von Daten durch Nutzer;
- zweckentfremdete Nutzung der Anwendungen von Microsoft 365;
- fehlerhafte Grundeinstellung des Systems durch den Administrator;
- Cyberangriff auf Microsoft 365;

---

<sup>8</sup> Siehe hierzu u.a. LfDI Rheinland-Pfalz, [FAQs zu Microsoft 365](#), zuletzt abgerufen: 30.01.2023; LfDI Baden-Württemberg, [Hinweise des LfDI Zur Nutzung von Microsoft 365 durch Schulen](#) (mit weiteren Anlagen), zuletzt abgerufen: 30.01.2023; Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt, [Hinweise zur Ausstattung der Schulen mit digitalen Endgeräten unter Nutzung von Produkten wie Microsoft Office 365](#), zuletzt abgerufen: 30.01.2023.

- Ausfall der Plattform aufgrund eines technischen Defekts.

Nachfolgend sollten die konkreten Risiken bezüglich des Einsatzes von Microsoft 365 innerhalb der öffentlichen Bildungseinrichtung ermittelt und umfassend begutachtet werden. Hierzu sollten nicht nur die einschlägigen Risikoszenarien dargestellt, sondern auch eine Bewertung sowohl der Eintrittswahrscheinlichkeit des Risikos als auch des jeweiligen Schadensausmaßes durchgeführt werden, um abschließend einen Risikowert gemäß der Risikomatrix bestimmen zu können.

Hierzu kann sich an folgendem Beispiel orientiert werden:

Beispiel-Risikobewertung: „Cyberangriff auf Microsoft 365“

Die Eintrittswahrscheinlichkeit für einen Angriff auf Microsoft 365 durch einen externen Angreifer kann als **substanziell** bewertet werden. Cyberangriffe sind – nicht zuletzt aufgrund einer mit der Corona-Pandemie einhergehenden verstärkten Auslagerung von analogen Prozessen in den digitalen Raum – eine ständige Bedrohung für Behörden, Unternehmen und staatliche Einrichtungen und kommen täglich vor. Zwar stehen öffentliche Bildungseinrichtungen – was die wirtschaftlichen Interessen von Angreifern betrifft – in der Regel hinter Unternehmen zurück. Die überaus große Zahl an Nutzern sowie die Tatsache, dass Angreifer nicht unbedingt spezifische Einrichtungen, sondern eine größtmögliche Angriffsfläche suchen, macht jedoch auch öffentliche Bildungseinrichtungen für Angreifer interessant.

Die Schwere des Schadens durch die aus einem Cyberangriff potenziell folgende unbefugte Offenlegung von und den Zugang zu Daten hängt maßgeblich von der jeweiligen Art der Daten ab, kann jedoch insgesamt – gerade mit Blick auf insbesondere Leistungs- und Personaldaten – als **substanziell** eingeordnet werden. Auch wenn andere verarbeitete Daten per se nur ein geringes Missbrauchsrisiko bieten, können sie in den Händen von Unbefugten für weitere Angriffe missbraucht werden.

<b>Schaden</b>	groß	4	8	12	16
	substanziell	3	6	9	12
	überschau- bar	2	4	6	8
	gering	1	2	3	4
	X	gering	überschau- bar	substanziell	groß
<b>Eintrittswahrscheinlichkeit</b>					

Die [Name der öffentlichen Bildungseinrichtung] hat im Rahmen der Bewertung des Einsatzes von Microsoft 365 die folgenden Risiken ermittelt und entsprechend begutachtet: [Beschreibung und Bewertung der konkreten Risiken im Einzelfall]

### 2.3.2 Gesamtrisiko

Hinweis: Aus der Einzelbetrachtung der Risiken ist ein Gesamtrisiko zu bilden. Hierzu werden die Risikowerte der ermittelten Einzelrisiken addiert und durch die Gesamtzahl der Einzelrisiken geteilt. Das Ergebnis stellt den Risikowert des Gesamtrisikos dar. Dieser Wert kann ebenfalls mithilfe der Risikomatrix dargestellt werden, wobei das berechnete Ergebnis ggf. aufzurunden ist.

Es gelten daher die folgenden Schritte zur Ermittlung des Gesamtrisikos:

1. Anzahl der ermittelten Einzelrisiken: 13
2. Summe der Risikowerte der Einzelrisiken: 85
3. Division der Summe der Einzelrisikowerte durch die Anzahl der Einzelrisiken:  $85/13 = 6,53$
4. Ermittlung des Gesamtrisikowertes durch Aufrunden des Ergebnisses der Division:  $6,53 \rightarrow 7$
5. Darstellung des Gesamtrisikowertes in der Risikomatrix

Aus der Einzelbetrachtung der Risiken ergibt sich ohne Abhilfemaßnahmen das folgende Gesamtrisiko für den Einsatz von Microsoft 365 an der verantwortlichen [*Name der öffentlichen Bildungseinrichtung*]: [*Gesamtrisikobewertung im Einzelfall*]

## **2.4 Ermittlung und Bewertung von Abhilfemaßnahmen (Art. 35 Abs. 7 lit. d) DSGVO)**

Hinweis: Nach Art. 35 Abs. 7 lit. d) DSGVO soll die DSFA auch „die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird“, enthalten. Die Ermittlung und Bewertung der Abhilfemaßnahmen sollten die folgenden Punkte umfassen:

- Ermittlung geeigneter Abhilfemaßnahmen und Beschreibung von deren Auswirkung auf die festgestellten Risiken
- Bewertung, inwieweit die Maßnahmen geeignet sind, die ermittelten Risiken zu minimieren und die Einhaltung der DSGVO sicherzustellen. Neben der Beschreibung der ergriffenen Abhilfemaßnahmen ist es für die anschließende Restrisikoanalyse von wesentlicher Bedeutung, wie sich die einzelnen Abhilfemaßnahmen auf die zuvor festgestellten Risiken auswirken.

### **2.4.1 Abhilfemaßnahmen zu den ermittelten Risiken**

Hinweis: Geeignete Abhilfemaßnahmen können sowohl technische oder organisatorische Maßnahmen sein wie z.B. die Nutzung einer Multi-Faktor-Authentifizierung oder die Einführung von verpflichtenden Nutzungsbedingungen und Datenschutzs Schulungen. Auch sind Maßnahmen von Microsoft oder sonstigen Dritten, wie z.B. das von Microsoft angekündigte EU Data Boundary, zu berücksichtigen, sofern sie zur Risikoreduzierung im Einzelfall geeignet sind. Als Abhilfemaßnahme können auch Entwicklungen auf politischer Ebene, die einen Einfluss auf eines der festgestellten Risiken haben, wie z.B. der Erlass der EO, genannt werden. Ob einzelne Maßnahmen erforderlich sind, bedarf einer rechtlichen Bewertung im Einzelfall.

Zu berücksichtigen ist zudem, dass einzelne Datenschutzaufsichtsbehörden konkrete

Abhilfemaßnahmen empfehlen, die in der DSFA begutachtet werden sollten.<sup>9</sup> In Betracht kommen u.a.:

- Nutzung eines Vertragswerks, das auf den aktuellen EU-SCC beruht;
- Verwendung pseudonymer Mailadressen/Accounts und das Verbot der Nutzung privater Microsoft-Accounts;
- Minimierung des Personenbezugs der verarbeiteten Daten;
- Betrieb von Microsoft 365 auf eigenen IT-Strukturen („On-Premises-Lösung“) (Verzicht auf Cloud-Speicherung, [APP.1.1.A12 des IT-Grundschutzkompodiums](#)) oder bei Stellen innerhalb des EWR, die nicht dem [US-CLOUD-Act](#) unterliegen;
- Unterbindung der Übertragung von Telemetriedaten mithilfe von produktseitig vorhandenen Konfigurationsmöglichkeiten bei Einsatz von Microsoft 365 („[Steuerelemente](#)“) bzw. dem darunterliegenden Windows-Betriebssystem;
- Unterbindung der Übermittlung von Telemetriedaten durch vertragliche, technische oder organisatorische Maßnahmen;
- Nutzung über einen vorkonfigurierten und abgesicherten Browser mit integrierten Schutzmaßnahmen zur weitestgehenden Anonymisierung/Gleichschaltung der Metadaten;
- Zwischenschaltung entsprechend vorkonfigurierter Terminal-Clients zur weitestgehenden Anonymisierung/Gleichschaltung der Metadaten;
- Bereitstellung datensparsam konfigurierter Endgeräte;
- Umleitung des Internetverkehrs über eine eigene Infrastruktur mit geeigneten technischen Maßnahmen zur Verschleierung der heimischen IP-Adressen;
- Prüfung der Datenübertragungen von Microsoft, u.a. mithilfe des [Diagnosedaten-Viewer](#) (DDV) von Microsoft;
- Überwachung von Microsoft-Produktupdates und Prüfung etwaiger damit verbundener Konfigurationsänderungen;
- Vereinbarung und Implementierung des EU Data Boundary von Microsoft sowie ggf. Ergreifen zusätzlicher technischer Lösungen.

Die Beschreibung der Abhilfemaßnahmen und deren Auswirkungen kann sich an dem

---

<sup>9</sup> Siehe hierzu u.a. LfDI Rheinland-Pfalz, [FAQs zu Microsoft 365](#), zuletzt abgerufen: 30.01.2023; LfDI Baden-Württemberg, [Hinweise des LfDI Zur Nutzung von Microsoft 365 durch Schulen](#) (mit weiteren Anlagen), zuletzt abgerufen: 30.01.2023.

folgenden Beispiel orientieren:

Beispiel: „Verwendung pseudonymer Mailadressen/Accounts und das Verbot der Nutzung privater Microsoft-Accounts“

Mit der Verwendung pseudonymer Mailadressen/Accounts und dem Verbot der Nutzung privater Microsoft-Accounts kann der Umfang der Datenverarbeitung in Microsoft 365 an einer öffentlichen Bildungseinrichtung erheblich minimiert werden. Damit können zunächst sämtliche Risiken, die mit dem Einsatz von Microsoft 365 an der jeweiligen Bildungseinrichtung in Verbindung stehen, reduziert werden. Durch den Einsatz der Pseudonymisierung und des Verbots der Nutzung privater Microsoft-Accounts kann darüber hinaus insbesondere das Risiko eines Überwachungseffekts der Nutzer erheblich gemindert werden. Auch wird durch den Einsatz von Pseudonymen und das Verbot der Privatnutzung der Anreiz für eine unbefugte Weitergabe der Daten durch andere Nutzer sowie die zweckentfremdete Nutzung von Microsoft 365 gemindert.

Die [Name der öffentlichen Bildungseinrichtung] hat als Verantwortliche die folgenden Abhilfemaßnahmen ergriffen: [Konkrete Beschreibung der Abhilfemaßnahme und deren Auswirkung]

#### **2.4.2 Abschließende Risikoanalyse unter Berücksichtigung der Abhilfemaßnahmen**

Hinweis: Zur Bestimmung des Restrisikowertes sind die Auswirkungen der Abhilfemaßnahmen auf die Einzelrisiken in einer Gesamtbetrachtung zu bewerten. Auf Grundlage dieser Gesamtbetrachtung ist das Restrisiko, das nach Implementierung der Abhilfemaßnahmen verbleibt, festzulegen und anhand der Risikomatrix darzustellen.

Die ergriffenen Maßnahmen müssen in der Gesamtschau eine effektive Abhilfe für die identifizierten Risiken darstellen. So sollten für alle ermittelten Risiken mehrere Abhilfemaßnahmen in Erwägung gezogen werden. Die gänzliche Entfernung eines Risikos wird nur in den seltensten Fällen und allenfalls einzelfallbezogen gelingen – dies ist jedoch auch nicht erforderlich. Entscheidend ist vielmehr, dass die Risiken unter die kritische Schwelle des hohen Risikos fallen. Zur abschließenden Risikoanalyse können nicht nur die evaluierten Abhilfemaßnahmen berücksichtigt werden, sondern auch etwaige Maßnahmen von Microsoft sowie etwaige aktuelle politische Entwicklungen. Aus dieser Gesamtschau ist dann anhand der

Risikomatrix zu bewerten, ob die Risiken auf ein datenschutzrechtlich vertretbares Maß reduziert werden können.

[Beschreibung der abschließenden Restrisikoanalyse]

## **2.5 Weitere Inhalte**

### **2.5.1 Nachhaltige Sicherung des Datenschutzes (Art. 35 Abs. 11 DSGVO)**

Hinweis: Zur Aufrechterhaltung des Datenschutzes ist der Einsatz von Microsoft 365 im Rahmen eines Datenschutzmanagements regelmäßig sowie anlassbezogen zu überprüfen (Art. 35 Abs. 11 DSGVO). Sollten z.B. einzelne Anwendungen für die genannten Zwecke nicht mehr oder nur noch in einem gewissen Umfang benötigt werden, könnten diese Anwendungen deaktiviert oder eingegrenzt werden. Hierbei sollten auch die Entwicklungen der Microsoft-365-Anwendungen berücksichtigt werden. Gleiches gilt für die regelmäßige Bewertung der zuvor ermittelten Datenschutzrisiken. Wir empfehlen, die DSFA spätestens in einem Zeitraum von zwei Jahren seit der Erstellung der DSFA regelmäßig zu überprüfen.

[Beschreibung der nachhaltigen Sicherung des Datenschutzes]

### **2.5.2 Anlagen**

Hinweis: Im Folgenden sollten sämtliche Anlagen in einem Anlagenverzeichnis aufgelistet werden. Als Anlagen kommen z.B. sämtliche Vereinbarungen mit Microsoft sowie alle Dokumente, auf die in der DSFA referenziert wurde, in Betracht.

[Auflistung aller Anlagen]