|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Verarbeitungstätigkeit: Benennung: \_\_Microsoft Office 365\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | lfd. Nr.: \_\_\_\_\_ |
| Datum der Einführung: | | | Datum der letzten Änderung: | |
| Verantwortliche Fachabteilung  Ansprechpartner  Telefon  E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a) | |  | | |
| Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b) | | **Durchführung von Unterricht, Teamarbeit im Kollegium,   Kommunikation** auf der Rechtsgrundlage von DS-GVO Art. 6 lit. a (Einwilligung):   §120 SchulG Abs. 2 Satz 2, 3, §121 SchulG Abs. 1 Satz 5 | | |
| Optional: Name des eingesetzten Verfahrens | | Arbeitsplattform/ Lern Management System (LMS) - **Office 365** | | |
| Beschreibung der  Kategorien betroffener  Personen  (Art. 30 Abs. 1 S. 2 lit. c) | | ☐ (1) Schüler  ☐ (2) Lehrkräfte | | |
| Beschreibung der Kategorien von personenbezogenen Daten  (Art. 30 Abs. 1 S. 2 lit. c) | | **Für die Verwaltung von Nutzern, Berechtigungen, Lizenzen**  ☐ (1, 2) Anmeldeinformationen, Rechte und Rollen, Zuteilung zu   Gruppen, Schulzugehörigkeit, Lizenzinformationen (Anzahl   Installationen; bei Nutzung von Office 365 Pro Plus]  **Vom Nutzer erzeugte Inhalte und Einstellungen**  ☐ (1, 2) Einwilligung Nutzungsbedingungen, persönliche Einstellungen,   Angaben in Nutzerprofil, vom Nutzer erstellte Inhalte, in die   Cloud gespeicherte Inhalte, E-Mail, Messages,   Kalendereinträge, Kommentare, Datenbankeinträge  ☐ (1) bei der Bearbeitung von Aufgaben gemachte Angaben, eingefügte   Inhalte, Antworten bei Tests, Anzahl (nicht) eingereichte Aufgaben,   Badges, erhaltenes Feedback  **Für die technische Funktionalität vom System erhobene Daten**  ☐ (1, 2) Geräte- und Nutzungsdaten (Gerätedaten nur bei BYOD und   außerschulischer Nutzung], Nutzungsdaten von Inhalten,   Interaktionen, Suchvorgänge und Befehle, Fehlermeldungen,   Sicherungskopien, [Positionsdaten - vor allem bei BYOD und   außerschulischer Nutzung relevant], Text-, Eingabe- und   Freihanddaten  Besondere Kategorien personenbezogener Daten (Art. 9):  ☐ | | |
| Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden  (Art. 30 Abs. 1 S. 2 lit. d) | ☐ intern (Zugriffsberechtigte)   * **Schulleitung** - alle Daten (1, 2) * **schulische Administratoren** - Nutzer- und Rechteverwaltung (1, 2) nach Anweisung durch die Schulleitung * **Lehrkräfte** - (1) Unterrichtsdaten soweit zur Durchführung des Unterrichts mit dem LMS erforderlich - nach Anweisung durch die Schulleitung * **Schüler** - eigene Daten und nach Freigabe die von Mitschülern, Nachrichten von Mitschülern | | | |
| ☐ extern   * **Microsoft** - auf der Grundlage von **Microsoft Volume Licensing Online Services Terms** vom *[Datum Vertragsabschluss]* * **Administrator IT Dienstleister**/ **Schulträger** - nach Anweisung durch die Schulleitung *[gegebenenfalls entsprechend Vertrag zur Auftragsverarbeitung mit … vom …]* * **Betroffene** nach Art. 15 DS-GVO | | | |
| ☐ Drittland oder internationale Organisation (Kategorie) | | | |
| ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)  Nennung der konkreten Datenempfänger | **☐** Datenübermittlung findet nicht statt und ist auch nicht geplant  **X** Datenübermittlung findet wie folgt statt:  **an Microsoft**  ☐ Drittland oder internationale Organisation (Name) | | | |
| Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt. | Dokumentation geeigneter Garantien  *laut Online Service Terms OST*   * EU-US Privacy Shield * Standardvertragsklauseln | | | |
| Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f) | **Durch die Schule**  (1, 2) Löschung der Zuordnungen von Lizenzen zu Benutzern am Ende der   Schulzugehörigkeit, in der Regel zum Ende des Schuljahres  **Durch Microsoft**  (1, 2) Löschung aller Daten im Zusammenhang mit dem Konto des   Benutzers 30 Tage nach Löschung der Zuordnung der Lizenz zum   Benutzer durch die Schule | | | |

# 

# Technische und organisatorische Maßnahmen

gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g)

Hier sind Maßnahmen aufgeführt, die für das Verfahren spezifisch sind, um Schutz und Sicherheit der verarbeiteten personenbezogenen Daten zu gewährleisten. Da viele übergreifende Maßnahmen bereits im schulischen Datensicherheitskonzept aufgeführt sind, werden hier nur die Maßnahmen aufgeführt, die mit Besonderheiten dieses Verfahrens zusammenhängen. Nicht jede Kategorie von Maßnahmen muss deshalb einen Eintrag haben.

|  |
| --- |
| 1. Pseudonymisierung |
| 2. Verschlüsselung |
| 3. Gewährleistung der Vertraulichkeit |
| 4. Gewährleistung der Integrität |
| 5. Gewährleistung der Verfügbarkeit |
| 6. Gewährleistung der Belastbarkeit der Systeme |
| 7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener  Daten nach einem physischen oder technischen Zwischenfall |
| 8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der  Wirksamkeit der technischen und organisatorischen Maßnahmen |
| Es liegen schriftlich vor:  * interne Verhaltensregeln: **Nutzungsvereinbarung** * allgemeines schulisches Datenschutzkonzept * übergreifendes schulisches Datensicherheitskonzept (*mit technischen und organisatorischen Maßnahmen*) * Wiederanlaufkonzept * schulisches Löschkonzept * Sonstiges: Durch Microsoft **Maßnahmen entsprechend den Anforderungen der ISO 27001, ISO 27002 und ISO 27018**. Außerdem OST **Anhang B – Sicherheitsmaßnahmen,** *siehe Online Service Terms (OST)*[[1]](#footnote-0) |

……………………………… …………………… ...........................................................

Verantwortlicher Datum Unterschrift   
✄-- D I E S E ---- S E I T E ---- G E H O E R T ---- N I C H T ---- Z U R ----- B E S C H R E I B U N G --

**Hinweise zum Ergänzen und Anpassen der Angaben**

* Die Beschreibung geht davon aus, dass Office 365 direkt genutzt wird, also nicht mit einer Single Sign-on Lösung.
* Bei einer Single Sign-on Lösung, die nur online genutzt wird, wäre **Pseudonymisierung** unter den Technischen und organisatorischen Maßnahmen aufzunehmen.
* Unter **Es liegen schriftlich vor**, sollte die **Nutzungsvereinbarung** erwähnt sein.
* Es ist zu empfehlen, die Zuständigkeiten für das Löschen der Zuordnungen von Nutzern und Lizenzen im schulischen **Löschkonzept** festzuschreiben.
* Liegt ein **übergreifendes schulisches Datensicherheitskonzept** vor, welches auch die Nutzung von Office 365 berücksichtigt, brauchen in die TOM Tabelle nur noch Maßnahmen eingetragen werden, die so speziell sind, dass sie dort nicht berücksichtigt sind.

1. "Licensing Terms | Microsoft Volume Licensing." entsprechend dem Datum des Vertragsabschlusses mit Microsoft <https://www.microsoft.com/en-us/licensing/product-licensing/products>. Accessed 7 Nov. 2018. [↑](#footnote-ref-0)