Kreis Offenbach

Vereinbarung über die Verarbeitung von Daten im Auftrag

zwischen

Schule
- Schulleitung -

-Auftraggeber / Verantwortlicher -

und

Kreisverwaltung Offenbach
vertreten durch Fachdienst Informationstechnologie
Werner-Hilpert-Str. 1
63128 Dietzenbach

- Auftragnehmer / Auftragsverarbeiter -

1. Allgemeines

(1) Zwischen dem Verantwortlichen gemäß Art. 4 Nr. 7 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) und dem Auftragsverarbeiter kommt eine Verarbeitung von Daten im Auftrag im Sinne der Art. 4 Nr. 8 und Art. 28 DSGVO zustande.

Diese Vereinbarung regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

(2) Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ im Sinne des Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Arten der personenbezogenen Daten und die Kategorien betroffener Personen sind in den jeweiligen **Anlagen zur Auftragsverarbeitung** zu dieser Vereinbarung festgelegt. Diese Anlagen können ebenfalls als Nachtrag zu dieser Vereinbarung über die Verarbeitung von Daten im Auftrag eingebunden werden.

3. Rechte und Pflichten des Verantwortlichen

(1) Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Verantwortlichen darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Verantwortliche ist für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Verantwortlichen unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z. B. E-Mail) erfolgen.

(4) Der Verantwortliche kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in den jeweiligen **Anlagen zur Auftragsverarbeitung** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Verantwortlichen ändern, wird der Verantwortliche dies dem Auftragnehmer in Textform mitteilen.

(5) Der Verantwortliche informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Verantwortlichen geltenden gesetzlichen Meldepflicht besteht, ist der Verantwortliche für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Verantwortlichen erteilten schriftlich ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach dieser Vereinbarung und/oder den Weisungen des Verantwortlichen. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Verantwortliche dieser schriftlich zugestimmt hat.

(2) Die Verarbeitung der Daten findet vorwiegend in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Die Verarbeitung personenbezogener Daten in ein Drittland darf nur erfolgen, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

Entsprechend wird das angemessene Schutzniveau entweder festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO), hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b) i. V. m. 47 DSGVO), hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c) und d) DSGVO), hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e) i. V. m. 40 DSGVO), hergestellt durch einen genehmigten

Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f) i. V. m. 42 DSGVO) oder wird hergestellt durch sonstige Maßnahmen gemäß Art. 46 Abs. 2 lit. a), Abs. 3 lit. a) und b) DSGVO).

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Verantwortlichen abstimmen.

(5) Der Auftragnehmer wird den Verantwortlichen unverzüglich darüber informieren, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Verantwortlichen zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Der Auftragnehmer wird die Daten, die er im Auftrag für den Verantwortlichen verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(7) Der Auftragnehmer kann dem Verantwortlichen die Person(en) benennen, die zum Empfang von Weisungen des Verantwortlichen berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in den jeweiligen **Anlagen zur Auftragsverarbeitung** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Verantwortlichen in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

(2) Die Kontaktdaten des benannten Datenschutzbeauftragten sind in der Anlage TOM, Abschnitt 4.1 hinterlegt.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Verantwortlichen jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Verantwortlichen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des

Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Verantwortlichen verarbeitet.

(2) Ferner wird der Auftragnehmer den Verantwortlichen unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Verantwortlichen erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Verantwortlichen eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Verantwortlichen bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Verantwortlichen insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Verantwortlichen verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Verantwortlichen muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Verantwortlichen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieser Vereinbarung.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Verantwortlichen mit. Er hat dem Verantwortlichen die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Verantwortliche hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Verantwortlichen durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(1a) Der Verantwortliche setzt für die Kontrollen im Sinne des Absatzes 1 entweder eigenes Personal oder externe Dienstleister ein, welche nicht gleichzeitig für Mitbewerber des Auftragnehmers tätig sind.

(2) Der Auftragnehmer ist dem Verantwortlichen gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle im Sinne des Absatzes 1 erforderlich ist.

(3) Der Verantwortliche kann eine Einsichtnahme in die vom Auftragnehmer für den Verantwortlichen verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Verantwortliche kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Verantwortliche wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Verantwortlichen i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Verantwortlichen zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Verantwortliche ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Verantwortlichen in Textform zulässig. Der Auftragnehmer stimmt der Nutzung der in den jeweiligen **Anlagen zur Auftragsverarbeitung** genannten Unterauftragsverhältnisse explizit zu.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Verantwortlichen und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Dauer der Vereinbarung zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Verantwortlichen zu übermitteln.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Verantwortlichen hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(4) Der Auftragnehmer hat sicherzustellen, dass die in dieser Vereinbarung vereinbarten Regelungen und ggf. ergänzende Weisungen des Verantwortlichen auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer eine Vereinbarung zur Auftragsverarbeitung zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen

Verantwortlichen und Auftragnehmer festgelegt sind. Dem Verantwortlichen ist die Vereinbarung zur Verarbeitung von Daten im Auftrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieser Vereinbarung) des Verantwortlichen und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Verantwortlichen und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Verantwortlichen erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Verantwortlichen verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Verantwortlichen obliegen. Der Verantwortlichen ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Verantwortlichen informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Verantwortlichen auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Verantwortliche ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Verantwortlichen bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Verantwortlichen erteilt werden,

damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Verantwortlichen erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Verantwortlichen treffen. Der Auftragnehmer wird den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieser Vereinbarung erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung der Vereinbarung zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Verantwortlichen zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage TOM** zu dieser Vereinbarung beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Verantwortlichen abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Verantwortlichen umgesetzt werden. Der Verantwortliche kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z. B. auch erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DS-GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Datenschutzbeauftragter) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001).

(4) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit

kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Verantwortlichen informieren.

14. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von drei Monaten zum Quartalsende durch den Verantwortlichen kündbar.

(3) Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Verantwortlichen oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

15. Beendigung

(1) Nach Beendigung der Vereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(2) Der Verantwortliche hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Verantwortlichen angekündigt werden.

16. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

17. Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Verantwortlichen unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen der Vereinbarung nicht.

Kreis Offenbach

_____,_____		Offenbach,	27.04.2022
Ort	Datum		Datum

- Verantwortlicher - - Auftragnehmer -

Anlage A zur Auftragsverarbeitung – Wartung pädagogisches Netzwerk

1. Gegenstand sowie Art und Zweck der Verarbeitung

Die Verarbeitung von Daten des Verantwortlichen durch den Auftragnehmer umfassen folgende Arbeiten und/oder Leistungen:

Gegenstand der Verarbeitung sind die Wartungs-, Pflege- und Supportleistungen einer von der Schule selbstständig beauftragten, pädagogischen IT-Cloudlösung auf Basis von Microsoft Office 365.

Die Datenverarbeitung innerhalb der Office 365 Plattform wird vertraglich zwischen dem Auftraggeber/Verantwortlichen und Microsoft Ireland Operations, Ltd. geregelt und ist nicht Bestandteil dieser Auftragsverarbeitung.

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten des Verantwortlichen sind nicht Zweck der Verarbeitung dieser Anlage A zur Auftragsverarbeitung – Wartung pädagogisches Netzwerk, kann aber zu dessen Erfüllung notwendig werden.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind können Gegenstand der Verarbeitung werden:

- Anzeigename
- Familienname
- Vorname
- Externe ID
- Klasse
- Kurse
- Kursjahr bzw. Schuljahr
- E-Mailadresse
- Foto
- Technische Protokolldaten
- Stundenplan
- Benutzername
- Personenrolle
- Person
- Benutzergruppe
- Benutzerzugang (aktiv, gesperrt)
- Sprache
- E-Mailadresse
- Letzte Anmeldung
- OTP Schlüssel
- Office 365 Tenant ID
- Profileinstellungen
- Passwort (verschlüsselt)/Anmeldename

Zusätzlich bei Lehrkräften / nicht-unterrichtenden Personal:

- unterrichtete Fächer/Kurse
- unterrichtete Klassen
- dienstliche Telefonnummer
- Gruppenzugehörigkeit (z. B. Fachschaft)
- Protokollierung der Nutzung (kurzfristige Aufbewahrung)

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Alle Nutzer des pädagogischen Cloudsystems
- Personen, deren Daten im pädagogischen Cloudsystem verarbeitet werden, u. A.
- Schülerinnen und Schüler sowie deren Erziehungsberechtigte
- Lehrkräfte
- Sonstige Beschäftigte des Verantwortlichen

4. Unterauftragsnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Verantwortlichen Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Unterauftragnehmer	**Art der Leistung**
AnyDesk Software GmbH Türlenstraße 2 70191 Stuttgart	Nutzung eines Tools für den Remote-Support
Zammad GmbH Marienstraße 18 10117 Berlin	Nutzung eines Ticketsystems zum Management von Endnutzer- und Administratorenanfragen

5. Weisungsberechtigte Personen des Verantwortlichen

Weisungsberechtigt ist die Schulleitung bzw. deren Vertreter:innen.

6. Weisungsempfangsberechtigte Personen des Auftragnehmers

Schul-Administration des Kreises Offenbach im Rahmen der Aufgabenbewältigung.

Primärer Ansprechpartner:

Herr L. Manus
Fachdienst Informationstechnologie
Werner-Hilpert-Straße 1
63165 Dietzenbach

06074 8180-4469
l.manus@kreis-offenbach.de

Anlage TOM
Technische und organisatorische Maßnahmen des Auftragnehmers

Der Kreis Offenbach der als Verantwortlicher oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, habt die folgenden technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten.

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Alarmanlage	Schlüsselregelung / Liste
Chipkarten / Transpondersysteme	Empfang / Rezeption / Pförtner
Manuelles Schließsystem	Besucher in Begleitung durch Mitarbeiter
Sicherheitsschlösser	Sorgfalt bei Auswahl des Wachpersonals
Schließsystem mit Codesperre	Sorgfalt bei Auswahl Reinigungsdienste
Absicherung der Gebäudeschächte	
Türen mit Knauf Außenseite	
Videoüberwachung der Eingänge	

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Anti-Viren-Software Server	Erstellen von Benutzerprofilen
Anti-Virus-Software Clients	Zentrale Passwortvergabe
Anti-Virus-Software mobile Geräte	Richtlinie „Sicheres Passwort"
Firewall	Richtlinie „Löschen / Vernichten"
Intrusion Detection Systeme	Richtlinie „Clean desk"
Einsatz VPN bei Remote-Zugriffen	Allg. Richtlinie Datenschutz und / oder Sicherheit
Verschlüsselung von Datenträgern	Mobile Device Policy
Verschlüsselung Smartphones	Anleitung „Manuelle Desktopsperre"
Gehäuseverriegelung	
BIOS Schutz (separates Passwort)	
Automatische Desktopsperre	
Verschlüsselung von Notebooks / Tablet	

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte
Externer Aktenvernichter (DIN 32757)	Minimale Anzahl an Administratoren
Physische Löschung von Datenträgern	Datenschutztresor
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Verwaltung Benutzerrechte durch Administratoren

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Festlegung von Datenbankrechten
Mandantenfähigkeit relevanter Anwendungen	Datensätze sind mit Zweckattributen versehen

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung im getrennten und abgesicherten Systen (mögl. verschlüsselt)	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Email-Verschlüsselung	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
Einsatz von VPN	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Protokollierung der Zugriffe und Abrufe	Weitergabe in anonymisierter oder pseudonymisierter Form
Sichere Transportbehälter	Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Persönliche Übergabe mit Protokoll
Nutzung von Signaturverfahren	

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept (ausformuliert)
Feuerlöscher Serverraum	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Serverraum klimatisiert	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
USV	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
Schutzsteckdosenleisten Serverraum	Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	Getrennte Partitionen für Betriebssysteme und Daten
RAID System / Festplattenspiegelung	
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutz-Management im Einsatz	Kreis Offenbach Datenschutzbeauftragter Werner-Hilpert-Straße 1 63128 Dietzenbach 06074 8180-0 datenschutz@kreis-offenbach.de
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet)	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz et.al.	Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)
Anderweitiges dokumentiertes Sicherheitskonzept (…)	Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Eine Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
Einsatz von Virenscanner und regelmäßige Aktualisierung	Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
Endpoint Detection and Response (EDR)	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

4.4. Auftragskontrolle (Outsourcing an Dritte)
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen
Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
Schriftliche Weisungen an den Auftragnehmer
Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit
Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Pflicht zur Benennung
Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
Regelung zum Einsatz weiterer Subunternehmer
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus