TSC THÜRINGER SCHULCLOUD

Freistaat Thüringen Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

zwischen der

Bildungseinrichtung/Institution: Staatliche RS „Bürgerschule" Sonneberg
Straße, Hausnummer: Unterer Markt 4
PLZ, Ort: 96515 Sonneberg
vertreten durch die Leitung Fr. Astrid Morgenroth
- nachstehend Auftraggeber genannt -

und dem

Freistaat Thüringen
- vertreten durch
Thüringer Ministerium für Bildung, Jugend und Sport
Werner-Seelenbinder-Straße 7
99096 Erfurt
- dieses vertreten durch
Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien
Heinrich-Heine-Allee 2-4
99438 Bad Berka
vertreten durch den Direktor Herrn Dr. Andreas Jantowski
- nachstehend Auftragnehmer genannt -

1. Gegenstand des Vertrages

Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten im Rahmen der Thüringer Schulcloud (nachfolgend: TSC), welche ein Modul des Thüringer Schulportals (nachfolgend: TSP) ist. Der Auftraggeber nutzt das vom Auftragnehmer angebotene TSP sowie die TSC. Die TSC bietet eine zentrale Plattform, mit der die Nutzenden vorrangig im schulischen, aber auch in allen Bereichen des Thüringer Bildungssystems kollaborativ, unabhängig vom verwendeten Endgerät, arbeiten können. Damit die Nutzenden auf die TSC zugreifen können, ist es notwendig, dass zunächst eine Registrierung im TSP durchgeführt wird. Hierfür werden durch den Auftraggeber personenbezogene Daten von Nutzenden an den Auftragnehmer zur Auftragsverarbeitung übermittelt. Weitere Details zum Auftragsgegenstand ergeben sich aus der Bereitstellungsvereinbarung für die TSC. Eine Beendigung der gegenständlichen Auftragsverarbeitung bestimmt sich im Übrigen nach Ziffer 13 Abs. 2 dieses Vertrages.
Der Auftragnehmer verarbeitet in Erfüllung dieses Vertrages personenbezogene Daten für den Auftraggeber i.S.v. Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

2. Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen als Verantwortlicher der Verarbeitung im Sinne des Art. 4 Nr. 7 DSGVO i. V. m. § 2 II BDSG allein verantwortlich. Dieses gilt insbesondere für die Beurteilung der Zulässigkeit der Verarbeitung grds. gemäß Art. 6 Abs. 1 DSGVO sowie landesspezifischer Gesetze als auch für die Wahrung der Rechte der Betroffenen u.a. nach den Art. 12 bis 22 DSGVO.

(2) Die Inhalte dieses AV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen (IT-Systemen) im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Der Auftragnehmer ist für die Einhaltung der jeweils für ihn als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO einschlägigen Datenschutzvorschriften, insbesondere des Art. 28 DSGVO, verantwortlich.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3. Umfang, Art und Zweck der Verarbeitung personenbezogener Daten

Der Umfang, die Art und der Zweck einer etwaigen Verarbeitung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in Ziffer 1 beschriebenen Vertragsverhältnisse ergibt.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

4. Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO (Art.28 Abs.3 Satz 2 lit. c DSGVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung dokumentiert (siehe Anlage 2).

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 Satz 2 lit. c, Art. 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO, herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen, wie beispielsweise dem Stand der Technik entsprechende Verschlüsselungsmaßnahmen, umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Berichtigung, Sperrung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – zu verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der zuständigen Aufsichtsbehörde.
Hierzu gehören:
a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine Feststellung von relevanten Verletzungsereignissen ermöglichen.
b) die Verpflichtung, Verstöße des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen oder weiterer vom Auftragnehmer beauftragter Auftragsverarbeiter gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen, unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DSGVO.
c) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen der Aufsichtsbehörde.

(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitenden und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten.

(4) Der Auftragnehmer verpflichtet sich, den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person zu unterstützen, ihm in diesem Zusammenhang sämtliche relevanten Informationen zur Verfügung zu stellen und Anfragen von Betroffenen unverzüglich an den Auftraggeber weiterzuleiten.

(5) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 2 DSGVO. Des Weiteren stellt er das Verzeichnis auf

Anfrage der Aufsichtsbehörde zur Verfügung. Auf Anfrage des Auftraggebers stellt der Auftragnehmer dem Auftraggeber alle Angaben zur Verfügung, die zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DSGVO benötigt werden.

(6) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.

(7) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

7. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Beim Auftragnehmer ist ein Datenschutzbeauftragter, Heinrich-Heine-Allee 2-4, 99438 Bad Berka, +49 (36458) 56 288, datenschutzbeauftragter@thillm.de bestellt. Die jeweils aktuellen Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO - der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO und Anlage 2.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Dokumentation der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber.

8. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Das ThILLM ist durch den Freistaat Thüringen mit dem Betrieb des TSP und der TSC beauftragt. Zur Erfüllung seiner Pflichten bedient sich das ThILLM diverser Unterauftragnehmer, die in Anlage 3 mit ihrer jeweiligen Funktion angegeben sind. Die in Anlage 3 benannten Unterauftragnehmer stellen den bei Abschluss des Vertrages aktuellen Stand dar.

(2) Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige Genehmigung des Auftraggebers in Anspruch. Dies gilt in gleicher Weise für den Fall, dass weitere Unterauftragsverhältnisse durch Unterauftragnehmer begründet werden. Der Auftragnehmer stellt sicher, dass eine entsprechende Genehmigung des Auftraggebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt. Der Auftraggeber teilt dem Auftragnehmer innerhalb eines Monats nach Zugang der Mitteilung die Genehmigung oder den Einspruch unter Angabe von Gründen mit. Erfolgt innerhalb dieser Frist keine Mitteilung des Auftraggebers an den Auftragnehmer, gilt die Genehmigung als erteilt.

(3) Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung:
Im Fall einer allgemeinen Genehmigung informiert der Auftragnehmer den Auftraggeber immer mindestens 6 Wochen vor der Auslagerung über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(4) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

(5) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage 3 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Zustimmung für das Tätigwerden als erteilt, sofern der Auftraggeber einer Beauftragung von Unterauftragnehmern allgemein zugestimmt hat.

(6) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.
Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit

zwischen den Vertragspartnern dieses Vertrages sowie den beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Die Unterauftragnehmer sind in jedem Fall in der Anlage 3 aufzuführen.

9. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen und/oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

10. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Bereitstellungsvereinbarung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

11. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

12. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Bereitstellungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Methode und dem Zeitpunkt der Löschung.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13. Sonstige Vereinbarungen

(1) Ein Entgelt für diesen Auftrag wird nicht gefordert. Soweit der Auftraggeber nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeitenden. Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

(2) Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig diese Vereinbarung. Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

(3) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt die Vereinbarung im Übrigen unberührt. Anstelle der rechtsunwirksamen oder

nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 167 BGB geschlossen werden kann.

(4) Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf diese Vereinbarung. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für die Änderungen dieser Klausel.

(5) Es gilt das Recht der Bundesrepublik Deutschland.

(6) Die Parteien vereinbaren als Gerichtsstand den Sitz des für die Stadt Bad Berka zuständigen Gerichts.

Sonneberg, den 10.08.23

Auftraggeber
(Leitung der Bildungseinrichtung/
Institution)

Bad Berka, den 6/7/2023

Auftragnehmer
(Direktor ThILLM)

Anlage 1

Auflistung der personenbezogenen Daten und dem Zweck ihrer Verarbeitung, Art der Daten:

- Personenstammdaten
- Kommunikationsdaten
- Protokolldaten
- Zugehörigkeit zur Bildungseinrichtung/Institution
- Rolle in der TSC
- Gruppenmitgliedschaft (Klassen und Teams)
- Temporäre Daten in Chats und Videokonferenzen
- Passwort
- Erzeugte Pseudonyme, Ort der Verwendung

Kreis der betroffenen Personen:

- Lehrerinnen und Lehrer
- Schülerinnen und Schüler
- Angestellte der Bildungseinrichtung/Institution
- Weitere Personen, zum Beispiel Bildungsexperten oder Eltern
- Mitarbeitende des Auftragnehmers und der Unterauftragnehmer

Anlage 2

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

I. Vertraulichkeit

(a) Zutrittskontrolle
- dokumentierte Schlüsselvergabe an Mitarbeitende
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines ThILLM-Mitarbeitenden.
- gesicherter Serverraum

(b) Zugangskontrolle
- Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeitende vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert.
- Passwortrichtlinie ist vorhanden.

(c) Zugriffskontrolle
- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeitende des Auftragnehmers
- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.

(d) Datenträgerkontrolle
- Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht).
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden zerstört (geschreddert).

(e) Trennungskontrolle
- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

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

(a) Weitergabekontrolle
- Alle Mitarbeitende sind i. S. d. Art. 32 Abs.4 DSGVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Vorliegen eines Löschkonzeptes
- Verschlüsselung mobiler Datenträger

(b) Eingabekontrolle
- Eingabe und Änderungen der Daten werden protokolliert.

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

(a) Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
- Einsatz von Festplattenspiegelung bei allen relevanten Servern
- Monitoring aller relevanten Server
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage
- Dauerhaft aktiver DDoS-Schutz
- Einsatz von Softwarefirewall und Portreglementierungen
- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

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

- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DSGVO).
- Die Mitarbeitenden des Auftragnehmers werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.
- Das ThILLM hat einen Datenschutzbeauftragten bestellt.

Anlage 3

Liste der Unterauftragnehmer

Folgende Unterauftragnehmer werden im Rahmen weiterer Auftragsverarbeitung eingesetzt:

- topdev GmbH, Am Seegraben 2, 99099 Erfurt, Dienstleister TSP
- Dataport AöR, Altenholzer Straße 10 – 14, 24161 Altenholz, Dienstleister TSC
- Technische Universität Ilmenau, Ehrenbergstraße 29, 98693 Ilmenau, Bereitstellung Serverräume