THÜRINGER SCHULCLOUD

Freistaat Thüringen
Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

zwischen der Schule

Schulname: GS Johann Sebastian Bach
Straße/Hausnummer: Am Plan 1
PLZ/Ort: 99310 Arnstadt
vertreten durch die Schulleitung Frau Marion Schrickel
- nachstehend Auftraggeber genannt -

und dem

Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ff. ThILLM)
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. Der Auftraggeber nutzt die vom Auftragnehmer angebotene Thüringer Schulcloud. Die Thüringer Schulcloud bietet eine zentrale Plattform, mit der sowohl Lehrer/innen ihren Unterricht vorbereiten als auch Schüler/innen Lerninhalte vertiefen, nachschlagen und üben können. Die Schüler/innen und Lehrer/innen erhalten Benutzerkonten, mit denen sie unabhängig von den verwendeten Endgeräten auf die Thüringer Schulcloud zugreifen können. Hierfür werden durch den Verantwortlichen Daten von Teilnehmenden der Schulcloud an das ThILLM zur Auftragsverarbeitung übermittelt. Weitere Details zum Auftragsgegenstand ergeben sich aus der Bereitstellungsvereinbarung für die Thüringer Schulcloud. Eine Beendigung der gegenständlichen Auftragsverarbeitung bestimmt sich im Übrigen nach Ziffer 11.2 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 gemäß Art. 6 Abs. 1 DSGVO und § 57 ThürSchulG sowie für die Wahrung der Rechte der Betroffenen u.a. nach den Art. 12 bis 22 DSGVO.
(2) Die Inhalte dieses Auftragsverarbeitungsvertrages 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 zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe **Anlage 2**). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 Satz 2 lit. c, 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 Mitarbeitern 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: