Vertrag über Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 DS-GVO

Zwischen der Schule (nachfolgend Auftraggeber genannt) und Schulmanager Online GmbH, Nymphenburger Straße 86, 80636 München (nachfolgend Auftragnehmer genannt) wird folgender Vertrag geschlossen:

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus den Allgemeinen Geschäftsbedingungen ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten

Personenstammdaten, Kontaktdaten, Adressen, Daten zur Schullaufbahn, Zugehörigkeit zu Gruppen, Daten zum Schulbetrieb (z. B. Stunden- und Vertretungsplan, besuchter Unterricht), Login-Daten (Benutzername/E-Mail-Adresse, Passwort), Fehlzeiten (z. B. Krankmeldungen, Beurlaubungen), Daten zum Verhalten und Maßnahmen (z. B. Klassenbucheinträge, Nachsitzen), Buchungsdaten (z. B. Elternsprechtage, Sprechstunden, Wahlfächer), Leistungsdaten (z. B. Noten), Kommunikationsinhalte (z. B. Chat-Verläufe), Einwilligungen, Zahlungsdaten, Protokolldaten, Bestandsdaten, Inhaltsdaten, Kommunikationsdaten (z. B. IP-Adressen) sowie jegliche weitere Art von personenbezogenen Daten der unter "Kategorien betroffener Personen" genannten Personengruppen, die im Schulalltag anfallen bzw. die von der Schule oder einer Person, der die Schule Zugriff auf die Software gegeben hat, in Schulmanager Online eingegeben werden.

Art und Zweck der Datenverarbeitung

Entwicklung und Betrieb der Web-Plattform "Schulmanager Online"

Kategorien betroffener Personen

Lehrer und sonstige Mitarbeiter der Schule. Schüler sowie deren Eltern, Ausbilder und sonstige Erziehungsberechtigte. Nutzer der Software. Sonstige mit der Schule verbundene Personen.

Laufzeit

Die Laufzeit dieses Vertrags zur Auftragsverarbeitung richtet sich nach der Laufzeit des sich aus den AGB ergebenden Vertragsverhältnisses, sofern sich aus den Bestimmungen dieses Vertrags zur Auftragsverarbeitung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in den AGB und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
2. Die Weisungen werden anfänglich durch die AGB festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die in den AGB nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

   Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36

DS-GVO genannten Pflichten.

4. 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. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

   Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen (siehe Anhang 3).
7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist, dies vom Weisungsrahmen umfasst ist und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.
9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende - je nach Entscheidung des Auftraggebers - entweder herauszugeben oder zu löschen.

   Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
11. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 31 DS-GVO zur Zusammenarbeit mit der Aufsichtsbehörde nachzukommen.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu

informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber auf Anfrage die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

   Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem

Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der in den AGB vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

   Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Die zum Zeitpunkt des Vertragsabschlusses beauftragten Subunternehmer sind in Anhang 2 aufgelistet. Vor Hinzuziehung weiterer oder Ersetzung dieser Subunternehmer informiert der Auftragnehmer den Auftraggeber mit einer Frist von zwei Wochen.

   Der Auftraggeber kann der Änderung – innerhalb einer Frist von zwei Wochen – aus wichtigem datenschutzrechtlichen Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Widerspricht der Auftraggeber innerhalb der Frist, so kann der Auftragnehmer entscheiden, ob er die Leistung ohne die beabsichtigte Änderung erbringt oder die Leistungserbringung zum geplanten Termin der Änderung einstellt.
3. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen der Schrift- oder Textform, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den

Verzicht auf dieses Formerfordernis.

3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen der AGB vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht. Die Parteien vereinbaren, unwirksame Regelungen durch wirksame Regelungen zu ersetzen, die dem wirtschaftlichen oder sonstigen Zweck der Regelungen am nächsten kommen. Dies gilt entsprechend für den Fall einer Regelungslücke.
4. Es gilt deutsches Recht. Gerichtsstand für aus diesem Vertrag entstehende Rechtsstreitigkeiten ist das für München zuständige Gericht.
5. Sofern der Auftraggeber dem KDG (Gesetz über den Kirchlichen Datenschutz) bzw. dem DSG-EKD (EKD-Datenschutzgesetz) unterliegt, verpflichtet sich der Auftragnehmer dazu, die Vorgaben des KDG bzw. des DSG-EKD – analog zu denen der DSGVO – anzuerkennen und einzuhalten.
6. Sollte bereits ein Vertrag zur Auftragsverarbeitung oder ein Vertrag zur Auftragsdatenverarbeitung zwischen dem Auftraggeber und dem Auftragnehmer bezüglich der Software Schulmanager Online bestehen, so endet dessen Gültigkeit mit Inkrafttreten dieses Vertrags.

§ 9 Haftung

Auf Art. 82 DS-GVO wird verwiesen.

Die Haftung jeder Partei ist begrenzt auf die Höhe der Zahlungen, die der Auftragnehmer vom Auftraggeber in den 12 Monaten vor dem Ereignis, aus dem sich der Haftungsanspruch ergibt, erhalten hat.

Anhang 1: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Zutrittskontrolle

    - Der Zutritt ist per Schlüssel bzw. Transponder gesichert.
    - Ausgegebene Schlüssel bzw. Transponder werden in einer Liste festgehalten.

    - Außerhalb der Geschäftszeiten sind Türen und Fenster verschlossen.
    - Die mit dem Hosting beauftragten Subunternehmer sind in Anhang 2 aufgeführt. Diese werden dazu verpflichtet, Maßnahmen zur Zutrittskontrolle zu treffen.
2. Zugangskontrolle

    - Nutzer können auf Schulmanager Online nur mit einer Kombination aus Benutzernamen/E-Mail-Adresse und Passwort zugreifen. Davon

ausgenommen sind öffentliche Bereiche wie z. B. der Kalender.
- Es existiert eine Richtlinie für die Passwortkomplexität in Schulmanager Online, die softwareseitig implementiert ist.
- Hashing von gespeicherten Passwörtern.
- Der Zugriff auf den Anwendungsserver durch den Auftragnehmer per SSH ist durch ein Public-/Private Key-Verfahren geschützt.
- Mitarbeiterrechner, auf denen personenbezogene Daten verarbeitet werden, die unter diesen Vertrag fallen, sind mit einer Antivirensoftware ausgestattet.

- Passwortschutz von Bildschirmarbeitsplätzen.

3. Zugriffskontrolle

    - Die Zugriffsberechtigung für Produktivsysteme durch den Auftragnehmer ist auf einen kleinen Kreis von Mitarbeitern beschränkt.
    - Berechtigungskonzept

4. Trennungskontrolle

    - Produktiv-, Entwicklungs- und Testumgebungen sind voneinander isoliert.
    - Datensätze verschiedener Kunden werden in der Datenbank durch eine Mandanten-ID voneinander unterschieden

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

1. Weitergabekontrolle

    - Die Datenübertragung zwischen Server und Client ist per SSL verschlüsselt.

    - Ruft ein Nutzer die HTTP-Seite (ohne Verschlüsselung) auf, so wird er auf die HTTPS-Seite (mit Verschlüsselung) weitergeleitet.
    - Der Zugriff auf den Anwendungsserver durch den Auftragnehmer erfolgt SSH-Verschlüsselt sowie durch eine SSL-Verschlüsselte Weboberfläche.
    - Verschlüsselter E-Mail-Versand mittels Transportverschlüsselung.

2. Eingabekontrolle

    - Zu allen Datensätzen wird das Erstelldatum sowie das Datum der letzten Änderung gespeichert.
    - Differenzierte Benutzerberechtigungen für das Erstellen, Lesen, Ändern und Löschen von Datensätzen.

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

1. Verfügbarkeitskontrolle

    - Off-site Backups werden regelmäßig automatisiert erstellt.
    - Parallel laufen mehrere Instanzen des Anwendungsservers.

- Diese Instanzen werden, falls sie abstürzen, automatisch neu gestartet.
- Firewall
- Installation von Sicherheitsupdates

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

1. Datenschutz-Management
    - Mitarbeiter, die personenbezogene Daten, die unter diesen Vertrag fallen, verarbeiten, werden auf das Datengeheimnis verpflichtet.
    - Bestellung eines Datenschutzbeauftragten.
    - Zuständigkeiten für Datenschutz und Informationssicherheit sind definiert.
    - Regelmäßige interne Kontrolle der Sicherheitsmaßnahmen.
2. Incident-Response-Management
    - Mitarbeiterrechner, auf denen personenbezogene Daten verarbeitet werden, die unter diesen Vertrag fallen, sind mit einer Antivirensoftware ausgestattet.
    - Die Verantwortlichkeit für die Meldung von Sicherheitsvorfällen/Datenpannen ist klar geregelt.
3. Datenschutzfreundliche Voreinstellungen
    - Auswahl datenschutzfreundlicher Voreinstellungen, soweit dies für die geplanten Verarbeitungen relevant ist.
    - Off-site Backups werden verschlüsselt übertragen und gespeichert
4. Auftragskontrolle
    - Auswahl von Auftragnehmern unter Datenschutz- und Datensicherheitsaskpekten.
    - Abschluss einer Vereinbarung zur Auftragsverarbeitung.
    - Erfassung vorhandener Unterauftragsverarbeiter.

Anhang 2: Subunternehmer

Die nachfolgend beschriebenen Teilleistungen werden zum Zeitpunkt des Vertragsabschlusses von Subunternehmern durchgeführt:

dogado GmbH, Saarlandstraße 25, 44139 Dortmund

Hosting und Betrieb der Anwendung

Strato AG, Pascalstraße 10, 10587 Berlin

Hosting und Betrieb der Anwendung

ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf

Hosting und Betrieb der Anwendung

1&1 IONOS SE, Elgendorfer Straße 57, 56410 Montabaur

Hosting und Betrieb der Anwendung

infra.run Service GmbH, Wilhelmine-Gemberg-Weg 14, 10179 Berlin

Hosting und Betrieb der Anwendung

Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen

Hosting und Betrieb der Anwendung

SysEleven GmbH, Boxhagener Straße 80, 10245 Berlin

Hosting und Betrieb der Anwendung

Anhang 3: Ansprechpartner für Datenschutzfragen

Weisungsempfänger ist der Support von Schulmanager Online unter info@schulmanager-online.de. Weisungsgeber ist die vom Auftraggeber in der Weboberfläche als Ansprechpartner hinterlegte Person sowie die Schulleitung.

Datenschutzbeauftragter der Schulmanager Online GmbH
c/o activeMind AG
Potsdamer Straße 3
80802 München
Tel.: 089 / 919294900
Mail: datenschutz@schulmanager-online.de

Der Vertrag wurde am 16.07.2021 um 09:08 Uhr durch Eugen Blumenstock, Realschulrektor (Bildungszentrum Wildberg, Realschule mit bilingualem Zug) abgeschlossen.