Anlage zum Softwarevertrag für www.klassengeld.de, der Auftragsverarbeitungsvertrag gemäß DSGVO

zwischen der

Grundschule xyz
Musterstr. 1
99999 Bad Muster
- Verantwortlicher - nachstehend Auftraggeber genannt –

und der

infin GmbH, Waldbahnstr. 70, 83324 Ruhpolding
Registergericht Traunstein, HRB 24830
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Softwarevertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten« im Sinne des Art. 4 Nr. 1 DS-GVO) des Auftraggebers verarbeiten.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Gegenstand des Auftrages im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO ergibt sich aus dem Nutzungsvertrag für Software, auf den hier verwiesen wird, im Folgenden Leistungsvereinbarung genannt.
(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung. 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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten- bzw. -kategorien:

- Lehrer: Vorname, Nachname, E-Mail
- Schüler: Vorname, Nachname, Klasse, ID-Nummer
- Erziehungsberechtigte: Vorname, Nachname, E-Mail, IBAN, Mobilfunknummer (optional)

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
Kundendaten (Lehrer, Schüler, Erziehungsberechtigte)

3. Technisch-organisatorische Maßnahmen

(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. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 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 [Einzelheiten in Anlage 1].

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

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, 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, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. 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:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt: IITR Datenschutz GmbH, Dr. Sebastian Kraska, Marienplatz 2 in 80331 München. Telefon: +49 89 1891 7360, Mail: email@iitr.de.
b) Die 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, dürfen 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.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) 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.
f) 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.
g) 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.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. 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 oder die Entsorgung von Datenträgern 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. Beauftragt sind:

1. Firma Hetzner Online GmbH, https://www.hetzner.de/
   für WebHosting der Daten und Applikationen
2. Firma windata GmbH, https://www.windata.de/
   für das Auslesen der jeweiligen Schulkonten
3. Firma infin - Research & Development, https://www.infin.ro/
   für Programmierung und Produktentwicklung

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

7. 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 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 (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

8. 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.
- 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 Verletzungs-ereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- 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
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

9. 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.

10. 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 Leistungsvereinbarung – 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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(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.
(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Das Dokument ist maschinell erstellt und gültig ohne Unterschriften.

Anlage 1 – Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

1. Vertraulichkeit

Zutrittskontrolle
Die Geschäftsräume sind durch Sicherheitsschlösser gesichert, die in der Zeit von 17:00 Uhr bis 08:00 Uhr wochentags sowie an Wochenenden und Feiertagen die Zugangstüren verriegeln.
Jede betriebsfremde Person wird direkt bei Zugang zu den Geschäftsräumen nach dem Besuchsgrund gefragt und dann zum betreffenden Mitarbeiter geführt. Betriebsfremde Personen, die keinen erkennbaren und/oder plausiblen Grund für ihren Besuch nennen können, werden den Geschäftsräumen unverzüglich verwiesen und die Geschäftsführung wird über diesen Vorfall informiert. Es wird ein Besuchsprotokoll geführt. Schlüssel besitzen nur die Geschäftsführung sowie autorisierte Personen. Die Schlüsselausgabe wird protokolliert.

Zugangskontrolle
Die Erteilung von Berechtigungen zum Zugang zu Daten und Systemen wird ausschließlich durch die Geschäftsführung nach fachlichen Gesichtspunkten erteilt. Jeder Mitarbeiter erhält nur Zugriff auf die für die Erfüllung seiner fachlichen und organisatorischen Aufgabe notwendigen Daten an seinem Arbeitsplatz, welcher mit einem jeweils täglich aktualisierten Virenschutzprogramm geschützt ist.
Die Erteilung und der Entzug von Berechtigungen werden innerhalb der jeweiligen Softwareumgebung protokolliert. Das Protokoll besteht aus zwei Teilen: Protokolliert werden einerseits alle Veränderungen der Rechtevergabe. Andererseits werden in Form der Log-Vorgänge alle Nutzungszeiträume protokolliert. Zugriff haben die IT-Administration und die Geschäftsleitung.

Zugriffskontrolle
Ändert sich ein Aufgabengebiet eines Mitarbeiters so erfolgt eine Überprüfung, inwieweit bisherige Berechtigungen ausreichen bzw. ob bisherige Berechtigungen weiterhin notwendig sind. Im Bedarfsfall erfolgt dann eine entsprechende Verlagerung in Form einer Erweiterung bzw. Beschränkung der Zugriffsrechte. Durch die direkte und eindeutig abgrenzbare arbeitsvertragliche Verpflichtung in Verbindung mit der individuellen Zugriffsberechtigung auf die jeweils notwendigen Systeme und deren unverzügliche Anpassung an ggf. veränderte arbeitsvertragliche Verpflichtungen wird somit auch fortlaufend die jeweilige Notwendigkeit der individuellen Berechtigung überprüft. Dadurch, dass eine Berechtigung stets nur im Zusammenhang mit der fachlichen und organisatorischen Aufgabe genau definiert ist, stellt der Auftragnehmer sicher, dass stets nur erforderliche Berechtigungen eingeräumt werden.
Es existiert eine Passwortrichtlinie. Danach wird für Passwörter eine Mindestlänge von 8 Zeichen verlangt. Ferner wird eine Passwortkomplexität verlangt, die technisch erzwungen wird.

Trennungskontrolle
Alle relevanten Daten können programmgesteuert nur auftragsbezogen dargestellt und bearbeitet werden. Jeder Mitarbeiter sieht nur die zum Auftrag notwendigen Daten und kann diese nur auftragsgebunden verarbeiten. Wenn möglich werden Verarbeitungsdaten nur maschinell verarbeitet und kommen nicht zur Ansicht des Operators.
Kundenrelevante Daten werden pro Einzelfall erfasst und an den jeweiligen Kunden programmgesteuert übermittelt, wodurch eine Übermittlung an einen „falschen Kunden“ ausgeschlossen ist. Zudem hat kein Kunde Zugriff auf interne Systeme, sondern die Einzelfalldaten werden pro Fall an den Kunden übertragen, der dann Zugriff auf die Daten auf seinen eigenen Systemen hat.
Testsysteme/Produktivsysteme sind physikalisch immer voneinander getrennt. Es existieren unterschiedliche Accounts.

2. Integrität

Weitergabekontrolle
Personenbezogene Daten werden zwischen Auftraggeber und Auftragnehmer über eine SSL-verschlüsselte Web-Verbindung übertragen Die Daten werden während des Transports nach dem Stand der Technik verschlüsselt.
Nach Beendigung des Auftrags werden personenbezogene Daten, soweit diese zwischen Auftraggeber und Auftragnehmer ausgetauscht wurden, gelöscht. Eine Dokumentation der Löschung erfolgt durch maschinelle Protokollierung.

Eingabekontrolle
Durch die jeweilige Anwendungssoftware kann festgestellt werden, wer personenbezogene Daten wie eingegeben, verändert oder gelöscht hat.

Anlage 1 – Fortsetzung

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle
Es ist eine unterbrechungsfreie Stromversorgung (USV) im Einsatz. Die Serverräume sind klimatisiert. Feuer- und Rauchmeldeanlagen sind vorhanden und werden entsprechend den gesetzlichen Vorgaben turnusmäßig durch den Beauftragten für Arbeitsschutz überprüft. Eine Festplattenspiegelung ist im Einsatz. Tägliche Backups können im Falle des Datenverlustes eingespielt werden.

Rasche Wiederherstellbarkeit
Ein Notfallplan ist vorhanden. Dabei wird eine rasche Datenwiederherstellung konstruktiv durch die Nutzung einer modularen Plattform (Aufgaben werden unterschiedlichen physikalischen Systemen zugeteilt; jedes System ist zumindest zweifach vorhanden) gewährleistet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management
Die Unternehmensleitung hat Verantwortung für Datenschutz und Informationssicherheit übernommen („Leitlinie“). Die Beschäftigten werden innerhalb einer individuellen und persönlichen Schulung bei Antritt und Wechsel des fachlichen Aufgabenbereichs zum Datenschutz geschult. Im Rahmen des Arbeitsvertrages werden die Beschäftigten zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Ein Datenschutzbeauftragter ist benannt worden.
Es werden verschiedene Maßnahmen zur Umsetzung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) getroffen. Hierzu zählen: keine Massenexport-möglichkeiten; nur einzelfallbezogener Datenzugriff; keine Möglichkeit auf direkten Zugriff auf Datenspeicher/Datenquelle (Datenbank).

Incident-Response-Management
Die Mitarbeiter haben die Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten einzuhalten. Alle Mitarbeiter werden zum Datenschutzrecht belehrt und haben sich verpflichtet, Datenschutzverstöße unverzüglich dem direkten Vorgesetzten zu melden. Neben den zuvor geschilderten technischen Maßnahmen wird so sichergestellt, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
Der Auftragnehmer hat ein Datenschutzmanagementsystem (DSMS) sowie einen Prozess zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA) implementiert.
Darüber hinaus belehrt der Auftragnehmer die Mitarbeiter individuell zum Thema Datenschutz, um die Umsetzung der Vorgaben der DSGVO im Unternehmen zu gewährleisten.

Ohne Weisung des Auftraggebers wird keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO durchgeführt. Absprachen und Vereinbarungen werden in der Regel schriftlich getroffen und damit Einvernehmen zwischen den Parteien hergestellt. Der Auftragnehmer wird gemäß Art. 6 dieses Vertrages eine strenge Auswahl externer Dienstleister vornehmen, sich vorab von deren Leistungen und Integrität informieren und Nachkontrollen durchführen.