Vereinbarung zur Auftragsverarbeitung

zwischen dem/der

Schule St. Stephan Straubing-Alburg, Grund- und Mittelschule
Fröbelstraße 10, 94315 Straubing

- Verantwortlicher - nachstehend „Auftraggeber“ genannt -

und der

Dr. Josef Raabe Verlags GmbH
Rotebühlstr. 77, 70178 Stuttgart

- Auftragsverarbeiter - nachstehend „Auftragnehmer“ genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

aSc EduPage ermöglicht die Führung eines elektronischen Klassenbuches in der Schule. Es bietet ferner die Ansicht und Bearbeitung der Daten über mobile Endgeräte. aSc EduPage ermöglicht das Versenden und Publizieren von Vertretungsplänen und Stundenplänen an den betroffenen Personenkreis. Auch die Bewertung des Lernverhaltens und Lernerfolge können in EduPage erfasst werden.

> Die Verarbeitung beinhaltet das Hosting zur Speicherung aller für den Verfahrenszweck erforderlichen Daten sowie Werkzeuge zur Eingabe und Verarbeitung der Daten. Das Verfahren ist webbasiert. Eine lokale Speicherung von Daten oder Zwischendaten auf den verwendeten Endgeräten erfolgt nicht.

aSc Stundenplan wird zur Erstellung von Stunden- und Vertretungsplänen eingesetzt.

> Die Verarbeitung beinhaltet das Hosting zur Speicherung aller für den Verfahrenszweck erforderlichen Daten sowie Werkzeuge zur Eingabe und Verarbeitung der Daten.

(2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von sechs Wochen zum Vertragsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Technische Beratung und Unterstützung bei **aSc Stundenplan**

a) Führen eines individuellen Stundenkontos

b) Automatisches und manuelles Erstellen und Überprüfen von Stundenplänen

c) Verwalten von Vertretungsplänen

Darüber hinausgehende technische Beratung und Unterstützung bei **aSc EduPage**

d) Führen eines individuellen Arbeitszeitkontos

e) Weitergabe der Stundenpläne an die Beschäftigen auch auf mobilen Endgeräten

f) Dokumentation der geleisteten unterrichtlichen Tätigkeit der Lehrkräfte

g) Protokollierung der gestellten Hausaufgaben

h) Dokumentation der Leistungen und Noten der Schüler

i) Benachrichtigen und informieren von Lehrern, Schülern und deren Eltern

j) Austausch von Informationen zwischen Schule, ihren Schülern und deren Eltern

k) Ausgabe auf eine passwortgeschützte App, passwortgeschützte Internetseite

l) Führung eines elektronischen Klassenbuches

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. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind bei **aSc Stundenplan** folgende Datenarten/-kategorien:

a) Daten der Schule

Schulnummer, amtliche Schulbezeichnung, Adressdaten, organisatorische Verkettung mit anderer Schule, Schulart, Bildungsgänge [Ausbildungsrichtung, Fachrichtung,

Fremdsprachenprofil], Angebot für ganztägige Betreuung, Unterbringungsangebot, sonstige Zusatzangebote, informationstechnische Ausstattung, sonstige Ausstattung.

b) Daten der Lehrkräfte

(a) Grunddaten: Name, Vornamen, Anrede, Namensbestandteile, Namenskürzel, Geschlecht, Adressdaten, Kontaktdaten (Telefonnummer, Telefaxnummer, E-Mail, URL [Webkommunikation]), Amts-/Dienstbezeichnung, Rechtsverhältnis, Beginn/Ende des Dienstverhältnisses, reduzierende Stunden, Mehrarbeit, Unterrichtsmehrung/-minderung (Art und Umfang), Nebentätigkeitsstunden, Ermäßigung (Grund, Umfang, Dauer), Freistellung/Altersteilzeit, Beurlaubung, Abwesenheit, Längerfristiger Ausfall (Umfang; Grund), Sprechstundendaten, Postfach, Raum in der Schule, Einsatz als mobile Reserve

(b) unterrichtete Fächer: Stundenzahl, unterrichtete Fächer

(c) Anrechnungsstunden: Daten zur Beschäftigung und zum Einsatz (Art der Anrechnung, Stundenzahl, Funktion/Tätigkeit, Schule, Erläuterungen)

(d) Klassenleitung: Klassen, in denen die Lehrkraft (stellvertretende) Klassenleitung ist

(e) Lehrerbezogene Stundenplanvorgaben: Welche Klassen in welchen Fächern wie viele Stunden unterrichtet werden sollen, Stundenplanvorgaben (z.B. Minimal- und Maximalzahl der Unterrichtsstunden/Tag bzw. /Woche, minimale und maximale Stundenzahl in der Mittagspause, Maximalzahl von Stunden hintereinander, Stundenpräferenzen, Halbtage oder Tage) Raum (nur zu führen, wenn nicht die Klasse, sondern die Lehrkraft über einen Stammraum verfügt), Kennzeichen für besonderen Einsatz (z.B. Teilnehmer, Fachbetreuer, 14-tägiger Wechsel)

(f) Lehrerbezogene Vertretungsplanvorgaben: Präsenzstunden, nicht verfügbare Stunden, Dauer der Absenz, benötigte Zusatzstunden für Lehrkräfte, Absenzgrund (fester Schlüssel: dienstlich außer Haus, dienstlich im Haus, Klassenfahrt, Studienfahrt, Unterrichtsgang, Krankheit, Sonstiges), Bemerkungen zur Vertretung

(g) Historie über gehaltene Vertretungsstunden: Anzahl, Art, Datum

(h) Arbeitszeitkonto: Haben, Soll

Darüber hinaus sind bei **aSc EduPage** folgende personenbezogene Datenarten/-kategorien Gegenstand der Verarbeitung:

b) Daten der Lehrkräfte

(i) Lehrbefähigung: Fächer der Lehrbefähigung

(j) Beschäftigungsverhältnis: Schule, Schuljahr, Beschäftigungsverhältnis, Abordnung an nichtschulische Dienststelle, Nebentätigkeit, Ausbildungsabschnitt bei Lehrkräften im

Vorbereitungsdienst

c) Daten der Schüler

Name, Vorname, Geburtsdatum, Adressdaten, Geschlecht, Klassenzugehörigkeit, Zugang, Abgang, Bewertung des Lernverhaltens, Anwesenheit, Abwesenheiten, Fehlzeiten, Gruppenzugehörigkeit, Alter, Geburtsort, Nationalität, Religion, Jahrgang, Zweig und Fachorientierung, Interessengruppen, Praktikum bei Firma, Beginn der Schulzeit, Ende der Schulzeit, Gesundheitsbemerkungen (freiwillig), Abbruch des Studiums, Schulabschluss

d) Daten der Eltern: Adressdaten, Kontaktdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind bei **aSc Stundenplan** folgende:

Jede Lehrkraft, die im Folgenden, laufenden oder vergangenen Schuljahr an der Schule tätig sein wird/ist/war, Pädagogische Mitarbeiter oder temporäre Mitarbeiter, alle aktuell oder im vergangenen Schuljahr zur Nutzung des Programms berechtigten Personen.

Die Kategorien der durch die Verarbeitung betroffenen Personen sind bei **aSc EduPage** folgende:

a) Lehrkräfte, nicht unterrichtendes Personal, Verwaltungspersonal der Schule sowie externes Betreuungspersonal, das im Folgenden, laufenden oder vergangenen Schuljahr der Schule tätig sein wird/ist/war, alle aktuell oder im vergangenen Schuljahr zur Nutzung des Programms berechtigten Personen Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

b) Schüler

c) Eltern der Schüler und gesetzliche Vertreter

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 DS-GVO insbesondere in

Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO 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 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
Als Datenschutzbeauftragte(r) ist beim Auftragnehmer

Herr Michael, Mayer, Auditor/Datenschutzbeauftragter, +49 (07158) 5294,
mayer@ses-mayer.de bestellt.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 DS-GVO [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.

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

Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

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 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen.

(3) 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 DS-GVO 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 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.

11. Sonstiges

Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Für Nebenabreden ist die Schriftform erforderlich.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Auftraggeber: **Schule St. Stephan Straubing-Alburg, Grund- und Mittelschule** Fröbelstraße 10, 94315 Straubing	Auftragnehmer: **Dr. Josef Raabe Verlags GmbH** Rotebühlstr. 77, 70178 Stuttgart
	Stuttgart, den
Ort, Datum	Ort, Datum

Auftraggeber (Raimund Betz)	Auftragnehmer (Dr. Josef Raabe Verlags GmbH)

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen;

  Chipkarten-/Transponder-Schließsystem
  Sicherheitsschlösser

- **Zugangskontrolle**

  Keine unbefugte Systembenutzung;

  Authentifikation mit Benutzer und Passwort
  Einsatz von Anti-Viren-Software
  Einsatz von Firewalls
  Einsatz von Mobile Device Management
  Einsatz von VPN-Technologien
  Gehäuseverriegelung
  Benutzerberechtigungen verwalten
  Erstellen von Benutzerprofilen
  Passwortvergabe/Passwortregeln
  Protokollierung der Besucher /Besucherbereich
  Sorgfältige Auswahl von Reinigungspersonal
  Sorgfältige Auswahl von Sicherheitspersonal

- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems;

  Einsatz von Aktenvernichtern
  Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
  Physische Löschung von Datenträgern vor deren Wiederverwendung
  Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  Verschlüsselung von Datenträgern
  Anzahl der Administratoren auf das „Notwendigste“ reduzieren
  Erstellen eines Berechtigungskonzepts
  Passwortrichtlinie inkl. Länge und Wechsel
  Sichere Aufbewahrung von Datenträgern
  Verwaltung der Benutzerrechte durch Systemadministratoren

- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden;

  Trennung von Produktiv – und Testsystem
  Logische Mandantentrennung (softwareseitig)

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**

  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; Eine Pseudonymisierung erfolgt wo erforderlich und möglich im jeweiligen Verfahren im Rahmen der (verfahrens-)spezifischen technischen und organisatorischen Maßnahmen.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport;

  Einrichtung von VPN-Tunneln

- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind;

  Protokollierung der Eingabe, Änderung und Löschung von Daten
  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 Berechtigungskonzept

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust;

  Feuerlöschgeräte in Serverräumen
  Feuer- und Rauchmeldeanlagen
  Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
  Klimaanlage in Serverräumen
  Schutzsteckdosenleisten in Serverräumen
  Unterbrechungsfreie Stromversorgung (USV)
  Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
  Erstellen eines Backup- und Recoverykonzepts
  Erstellen eines Notfallplans
  Testen von Datenwiederherstellung
  Serverräume nicht unter sanitären Anlagen

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**

  Backup-Strategie

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

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

- **Auftragskontrolle**
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers;

  Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
  Laufende Überprüfung des Auftragsnehmers und seiner Tätigkeit
  Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) (Art. 26 DS-GVO)
  Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
  Verpflichtung der Mitarbeiter des Auftragsnehmers auf das Datengeheimnis (§5 BDSG)

Firma Unterauftragnehmer	Anschrift/Land	Leistung
aSc Applied Software Consultants s.r.o.	Svoradova 7, 81103 Bratislava, Slowakei	Die Daten werden im Auftrag des Auftragnehmers (Dr. Josef Raabe Verlags-GmbH, Rotebühlstraße 77, 70178 Stuttgart) von aSc Applied Software Consultants verarbeitet. aSc Slowakei, entwickelt und verbessert die Software und kann zu diesem Zweck pseudonymisierte Daten verwenden. aSc Slowakei hat die Rolle der Entwicklung und des nachgelagerten Supports. Bei **aSc EduPage** werden die Daten im Auftrag des Unterauftragnehmers (aSc Applied Software Consultants s.r.o., Svoradova 7, 81103 Bratislava, Slowakei) auf Servern eines deutschen Serviceproviders (Hetzner AG, Industriestraße 25, 91710 Gunzenhausen) gehostet. Der Serviceprovider betreibt die Daten in einer gesicherten und nach ISO 27001:2013 zertifizierten Management-Systemumgebung im Auftrag des Unterauftragnehmers