Vertrag zur Auftragsverarbeitung

Zwischen

- Auftraggeber -

- vertreten durch -

und der

- Auftragnehmer -

Gemeinnütziges Berufsförderungswerk des Baden-Württembergischen Zimmerer- und Holzbaugewerbes GmbH
Bildungszentrum Holzbau
Leipzigstr. 13
88400 Biberach an der Riß

- vertreten durch Herr Jochen Ströhle -

wird folgender Vertrag geschlossen:

Präambel

(1) Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem jeweils gültigen ***Nutzungsvertrag BLok*** zwischen den o.g. Vertragsparteien ergeben. Dieser findet auf alle Tätigkeiten Anwendung, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

(2) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutzgrundverordnung (im Folgenden „DSGVO") zu verstehen.

(3) Soweit Erklärungen, Informationen und Dokumentationen „schriftlich" zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

Vertrag zur Auftragsverarbeitung

HOLZBAU BADEN-WÜRTTEMBERG BILDUNGSZENTRUM

Inhalt

§ 1 Gegenstand, Ort und Dauer des Vertrages 2
§ 2 Rechte und Pflichten des Auftraggebers 4
§ 3 Pflichten des Auftragnehmers 5
§ 4 Umsetzung von Betroffenenrechten oder Maßnahmen der Aufsichtsbehörden 6
§ 5 Kontrollrechte und -pflichten 7
§ 6 Mitteilungspflichten des Auftragnehmers 8
§ 7 Unterauftragsverhältnisse mit Subunternehmern 8
§ 8 Datensicherungsmaßnahmen nach Art. 32 DSGVO 10
§ 9 Löschung 11
§ 10 Vergütung 11
§ 11 Haftung 11
§ 12 Sonstiges 12

1 Gegenstand, Ort und Dauer des Vertrages

(1) Der Auftrag umfasst folgende Arbeiten:

Bereitstellung und Hosting des Softwaresystems BLok – Online-Berichtsheft

(2) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

(3) Art und Zweck der Verarbeitung (vgl. Art. 4 Nr. 2 DSGVO)

Durch den Auftragnehmer werden Daten im Rahmen der für eine Prüfungszulassung notwendigen Berichtsheftführung verarbeitet; dies betrifft die Daten der beteiligten Akteure, die in der Wochendokumentation erfassten Tätigkeiten und Fertigkeiten, sowie die zur Verbesserung der Dokumentation gespeicherten Dokumente. Alle prüfungsrelevanten Daten können optional durch den Nutzer der Kammer bereitgestellt werden.

Eine weitere konkrete Form der Verarbeitung personenbezogener Daten ist nicht beauftragt. Es sind alle Verarbeitungen zulässig, welche für die konkreten Betriebs-, Wartungs- und Supportvorgänge für den Auftraggeber erforderlich sind und den folgenden Regelungen entsprechen. Eine Verarbeitung der Daten des Auftraggebers auf andere Arten oder für andere Zwecke ist nicht zulässig.

(4) Art der personenbezogenen Daten (vgl. Art. 4 Nr. 1, sowie ggf. Nr. 13 bis 15 DSGVO)

Gegenstand der Verarbeitung personenbezogener Daten sind insbesondere folgende Datenarten / -kategorien:

- Profildaten
  - Kammer, Berufsschule, Ausbildungsbetrieb
  - Anrede, Name, Vorname
  - Geburtsdatum
  - E-Mail-Adresse
  - Beruf, Ausbildungszeitraum, Ausbildungsordnung, Rahmenlehrplan
  - Benutzername, Passwort
- Berichtsheft-Daten
  - Abteilung, Lernort, Status

  - Tätigkeiten, Erwartungserfüllung, Zeitdauer, Bemerkungen
  - Freigabedatum, freigebender Auszubildender
  - Abnahmedatum, kontrollierender Ausbilder
- Entwicklungsportfolio-Daten
  - Entwicklungsstand-Daten
  - Hochgeladene Dokumente
  - Einschätzungen zu personalen Fähigkeiten
  - Checklisten-Daten
- Kommunikationsdaten
  - Interne Nachrichten
  - Kommentare
  - Systemnachrichten per Mail

(5) Kategorien betroffener Personen (vgl. Art. 4 Nr. 1 DGVO)

- Beschäftigte
  - Mitarbeiter, insb. Ausbilder und Auszubildende
- Partner
  - Überbetriebliche Ausbilder

(6) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(7) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in den Geschäftsräumen des Auftragnehmers bzw. seiner Subunternehmen gemäß § 7 dieser Vereinbarung erfüllt.

(8) Das Vertragsverhältnis beginnt am Tag der Vertragsunterzeichnung. Es wird auf unbestimmte Zeit geschlossen und kann mit einer Frist von 3 Monaten zum Monatsende schriftlich gekündigt werden.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist schriftlich kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung, wie in diesem Abschnitt beschrieben, berechtigt.

Den Vertragspartnern ist bewusst, dass ohne Vorliegen eines gültigen Vertrages zur Auftragsverarbeitung keine (weiteren) Verarbeitungen durch den Auftragnehmer erfolgen dürfen.

2 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 DSGVO (sowie ggf. Art. 9 DSGVO) sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Eine Umsetzung durch den Auftragnehmer erfolgt nur auf ausdrückliche Weisung des Auftraggebers.

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt. Der Auftraggeber ist berechtigt, im Rahmen des Auftrags Einzelweisungen zu erteilen. Dem Auftraggeber ist bekannt, dass der seitens des Auftragnehmers bereitgestellte und im ***Nutzungsvertrag BLok*** vereinbarte Dienst weiteren Kunden des Auftragnehmers zur Verfügung steht (Cloud-Dienst). Der Auftraggeber wird dies berücksichtigen, insbesondere Weisungen so gestalten, dass sie ohne Beeinträchtigung anderer Einrichtungen umsetzbar sind. Falls Weisungen des Auftraggebers erheblichen Zusatzaufwand verursachen, wird der Auftragnehmer hierauf hinweisen. Hält der Auftraggeber an der Weisung fest, wird der Auftraggeber den entstandenen Aufwand angemessen vergüten.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. In begründeten Einzelfällen können durch Bevollmächtigte des Auftraggebers Weisungen auch mündlich erteilt werden. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre zu Nachweiszwecken aufzubewahren.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Die Vertragsparteien vereinbaren Weisungsberechtigte und für die Annahme von Weisungen folgende Ansprechpartner:

Weisungsberechtigte Personen des Auftraggebers sind:

Vor- und Nachname:

Organisationseinheit:

Telefonnummer:

E-Mail:

Weisungsempfänger beim Auftragnehmer ist:

Vor- und Nachname:	Jochen Ströhle
Organisationseinheit:	Ausbildung
Telefonnummer:	07351/44091-53
E-Mail:	j.stroehle@zimmererzentrum.de

Bei einem Wechsel oder einer Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich schriftlich oder in einem dokumentierten elektronischen Format die Nachfolger bzw. Vertreter mitzuteilen.

3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Eine darüber hinausgehende Verarbeitung ist nur in dem Umfang zulässig, in dem der Auftragnehmer zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftraggeber unterliegt, verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet (vgl. Art. 28 Abs. 3 Satz 2 a DSGVO).

Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige Vervielfältigungen, Sicherheitskopien (soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind) sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(2) Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(3) Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

(4) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften bekannt sind.

(5) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (vgl. Art. 28 Abs. 3 Satz 2b, Art. 29 DSGVO). Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind in angemessenen Abständen zu wiederholen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(6) Der Auftragnehmer hat folgende Person als Beauftragten für den Datenschutz bestellt:

Vor- und Nachname:	Jochen Ströhle
Organisationseinheit:	Datenschutzbeauftragter
Telefonnummer:	07351/44091-53
E-Mail:	j.stroehle@zimmererzentrum.de

Der Auftragnehmer stellt sicher, dass dieser die gesetzlichen Anforderungen erfüllt, insbesondere über eine angemessene Fachkunde verfügt. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. Der Auftraggeber kann sich in Datenschutzfragen direkt an den Datenschutzbeauftragten wenden.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich unter Nennung der dann gültigen Kontaktdaten mitzuteilen.

4 Umsetzung von Betroffenenrechten oder Maßnahmen der Aufsichtsbehörden

(1) Der Auftragnehmer ist verpflichtet, Anfragen betroffener Personen (insbesondere zur Geltendmachung ihrer Rechte nach Art. 12 bis 22 DSGVO) - sofern eine Zuordnung an den Auftraggeber aufgrund der Angaben durch die betroffene Person ggf. mittels angemessener Rückfragen möglich ist - unverzüglich an den Auftraggeber in dokumentierter Form weiterzuleiten.

(2) Bei der Erfüllung der Rechte der betroffenen Personen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen durch den Auftraggeber hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (vgl. Art. 28 Abs. 3 Satz 2 e, f DSGVO). Er hat die dazu erforderlichen Angaben und Dokumentationen vorzuhalten und dem Auftraggeber auf Anforderung an die benannten weisungsberechtigten Personen des Auftraggebers weiterzuleiten.

(3) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

(4) Der Auftragnehmer sichert Unterstützungsleistungen bzgl. Löschung von Benutzerkonten und damit verbundener Daten, Recht auf Vergessenwerden, Berichtigung von Benutzerattributen und Datenportabilität im PDF-Format sowie Auskunft nach dokumentierter Weisung des Auftraggebers zu.

(5) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(6) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder betroffene Personen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den

Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

5 Kontrollrechte und -pflichten

(1) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (siehe Anlage 1 – Technische und organisatorische Maßnahmen bei der Auftragsverarbeitung gemäß Art. 32 DSGVO) sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(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 Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber unter Berücksichtigung der Festlegungen in den folgenden Absätzen 4 und 5 jederzeit berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften, Nachweisen und die Einsichtnahme in die gespeicherten Daten des Auftraggebers und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort in dem Geschäftsbetrieb des Auftragnehmers (Art. 28 Abs. 3 Satz 2 h DSGVO). Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(4) Der Nachweis von Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann insbesondere wie folgt erfüllt werden:

- 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).

Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Widerruf eines o.g. Nachweises unverzüglich zu informieren.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Der Auftragnehmer darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten und organisatorischen Maßnahmen abhängig machen.

(6) Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung (in der Regel zwei Wochen

vor dem avisierten Termin) und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, sollen sich anlasslose Kontrollen auf Stichproben beschränken.

(7) Der Auftragnehmer ist nicht berechtigt, für die gesetzlich verpflichtende Durchführung von Kontrollen vom Auftraggeber eine Vergütung zu verlangen. Davon betroffen sind insbesondere regelmäßige Kontrollen im Sinne von Art. 28 Abs. 3 lit. h) DSGVO und Kontrollen bei berechtigtem Anlass (Anfangsverdacht). Für die Durchführung von darüber hinaus gehenden anlasslos durchgeführten Vor-Ort-Kontrollen kann der Auftragnehmer dagegen vom Auftraggeber eine angemessene Vergütung verlangen. Die Vergütung richtet sich nach der zum Zeitpunkt der Vor-Ort-Kontrolle jeweils aktuellen Preisliste des Auftragnehmers.

(8) Die Verarbeitung von Daten ist nur auf vom Auftragnehmer geprüften und den zur Auftragsverarbeitung eingesetzten Personen durch den Auftragnehmer bereitgestellten Endgeräten zulässig.

6 Mitteilungspflichten des Auftragnehmers

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt insbesondere auch in Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33, 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33, 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 f DSGVO). Meldungen für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(3) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten 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.

7 Unterauftragsverhältnisse mit Subunternehmern

(1) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice Dritter und die Entsorgung von Datenträgern des Auftragnehmers sind nicht erfasst. 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) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, andernfalls unzulässig. Der Auftragnehmer informiert hierzu den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer unter Angabe

von Namen und Anschrift sowie der vorgesehenen Tätigkeit des Subunternehmers, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO). Ist nach einer Frist von 4 Wochen ab Versand der Änderungsinformation kein begründeter Einspruch (schriftlich oder in einem dokumentierten elektronischen Format), i.S. des Abs. 8 erhoben wurden, dann gilt eine angezeigte Änderung als genehmigt.

(3) Eine Beauftragung von Subunternehmen in Drittstaaten darf darüber hinaus nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der europäischen Kommission, EU-Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(4) Darüber hinaus muss der Auftragnehmer vor Einschaltung eines Subunternehmens dafür Sorge tragen, dass er den Subunternehmern unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

(5) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und 9 DSGVO). In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmer. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen – auch vor Ort im Geschäftsbetrieb – bei den Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(6) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(7) Die relevanten Prüfunterlagen und Dokumentationen des Auftragnehmers sind dem Auftraggeber zur Verfügung zu stellen. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

(8) Eine Verweigerung der Genehmigung bedarf einer angemessenen Begründung des Auftraggebers (schriftlich oder in einem dokumentierten elektronischen Format) aus datenschutzrechtlicher Sicht. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist keine einvernehmliche Lösung zwischen den Parteien möglich, steht dem Auftraggeber ein Sonderkündigungsrecht zu. Eine bereits erteilte Genehmigung kann durch den Auftraggeber zurückgezogen werden, wenn die Genehmigung aufgrund falscher Informationen seitens des Auftragnehmers bzw. des Subunternehmers erteilt wurde bzw. die in diesem Vertrag geregelten Anforderungen an die Beauftragung nicht eingehalten werden.

(9) Die Weitergabe von personenbezogenen Daten des Auftraggebers an die Subunternehmer und deren erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(10) Die für den Auftragnehmer mit den Verarbeitungen von personenbezogenen Daten des Auftraggebers beschäftigten Subunternehmer werden in der ***Anlage 2 - Subunternehmen***

mit Name, Anschrift und Auftragsinhalt geführt. Mit deren Beauftragung erklärt sich der Auftraggeber im dargestellten Umfang einverstanden.

8 Datensicherungsmaßnahmen nach Art. 32 DSGVO

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO (Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit) in Bezug auf die konkrete Verarbeitung derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) 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. Ist keine einvernehmliche Lösung zwischen den Parteien möglich, steht dem Auftraggeber ein Sonderkündigungsrecht zu.

(3) Das in der Anlage 1 - Technische und organisatorische Maßnahmen bei der Auftragsverarbeitung gemäß Art. 32 DSGVO beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

(4) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 d DSGVO).

(5) Die Maßnahmen beim Auftragnehmer können und sollen im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei dürfen aber die vereinbarten Standards nicht unterschritten werden.

(6) Wesentliche Änderungen sind durch beide Parteien schriftlich zu vereinbaren. Die entsprechenden Informationen bzw. Vereinbarungen sind für die Dauer des Vertrages zu Nachweiszwecken aufzubewahren.

9 Löschung

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten einschließlich Backups, Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, vollständig datenschutzgerecht zu löschen bzw. zu vernichten; das Recht des Auftraggebers, gemäß § 2(2) des Nutzungsvertrags BLok zuvor die Herausgabe der Daten zu verlangen, bleibt hiervon unberührt. Daten innerhalb des Anwendungssystems BLok werden entsprechend dem jeweils gültigen Löschkonzept behandelt. Die Löschung/Vernichtung ist dem Auftraggeber mit Angabe von Ort, Zeit, Art der Durchführung und durchführender Person schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen (Vernichtungs- bzw. Löschprotokoll). Sämtliche beim Auftragnehmer vorhandene Kopien der Daten sind datenschutzkonform zu löschen/vernichten. Die Löschung von Daten aus den gemäß den Leistungsbeschreibungen erstellten Backups erfolgt im Rahmen der definierten Regellöschungsfristen nach Beendigung der Vorhaltezeit.

(2) Test- und Ausschussmaterialien sind vom Auftragnehmer unverzüglich zu löschen, sobald diese zur Erfüllung des Vertrages nicht mehr erforderlich sind und der Auftraggeber nicht ausdrücklich die Aushändigung der Materialien fordert.

(3) Eine Aufbewahrung bzw. Speicherung von Daten und Unterlagen durch den Auftragnehmer ist nur im Rahmen einer gesonderten Vereinbarung mit dem Auftraggeber oder im Rahmen einer Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig (Art. 28 Abs. 3 f DSGVO). Sind aufgrund gesetzlicher Vorgaben, oder aufgrund entgegenstehender gesetzlicher Pflichten zur Speicherung, Löschungen nicht zulässig, werden die entsprechenden Daten durch den Auftragnehmer in der Verarbeitung eingeschränkt (insbesondere durch Sperrung) und sicher unter Verschluss gehalten.

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

(5) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

10 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im jeweils gültigen Nutzungsvertrag BLok geregelt.

11 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 28 Abs. 4 und Abs. 10 und Art. 82 DSGVO getroffenen Regelungen.

12 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Satz 1 gilt nicht für Informationen, die allgemein zugänglich sind oder auf deren Vertraulichkeit der Auftraggeber oder der Auftragnehmer schriftlich verzichtet haben. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend für drei volle Kalenderjahre zu Nachweiszwecken aufzubewahren.

(3) Ergänzungen und Änderungen dieser Vereinbarung bedürfen der Schriftform.

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

(5) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(6) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist Chemnitz, Deutschland.

Biberach, ...	
Ort, Datum	Ort, Datum
.....	.....
Unterschrift Auftragnehmer	Unterschrift Auftraggeber
Ströhle, Jochen	
Name, Vorname in Klarschrift	Name, Vorname in Klarschrift
Ausbildung	
Funktion in Klarschrift	Funktion in Klarschrift
.....	.....
Stempel	Stempel

Anlage 1 - Technische und organisatorische Maßnahmen bei der Auftragsverarbeitung gemäß Art. 32 DSGVO

1. Sicherstellung von Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen
Die Datensicherung erfolgt mittels eines Backup-Verfahren (siehe Vertrag).
Die Server-Systeme werden auf virtualisierten, verteilten Servern betrieben.
Eine unterbrechungsfreie Stromversorgung (USV) ist gegeben.
Eine Firewall ist vorhanden.
Ein Notfallplan für Systemausfälle ist vorhanden.
Der Serverraum verfügt über Geräte zur Überwachung von Temperatur und Feuchtigkeit.
Es existieren Feuer- und Rauchmeldeanlagen.
Es sind Klimaanlagen vorhanden.

Sicherstellung der Belastbarkeit

Maßnahmen
Der Betrieb des Systems erfolgt auf leistungsfähiger, redundant ausgelegter Servertechnik.
Das Rechenzentrum verfügt über eine Breitband-Internetanbindung (DFN-Anbindung).
Es erfolgt eine kontinuierliche Überwachung von metrischen Daten der Systemserver (siehe IT-Sicherheitskonzept).

2. Sicherstellung der Integrität

Weitergabekontrolle

Maßnahmen
Die Datenübertragung erfolgt nicht auf physischen Datenträgern.
Die Datenübertragung im Internet erfolgt über verschlüsseltes http (https).
Datenübertragung im Zusammenhang mit Backups oder sonstigen Administrativen Tätigkeiten (beim Auftragnehmer) finden generell über ein getunneltes VPN (Virtuell Privat Network) statt.
Eine Datenübermittlung personenbezogener Daten an Dritte durch den Auftragnehmer selbst erfolgt nicht.

Eingabekontrolle

Maßnahmen
Alle Dateneingaben in das Anwendungssystem BLok werden dem entsprechenden Benutzer zugeordnet und sind daher nachvollziehbar.
Aussagen über die durchgeführten Änderungen an den Server-Systemen (Gründe, Zeitpunkt u. Ergebnis) sind schriftlich hinterlegt und können im Bedarfsfall ausgewertet werden.
Zugriffe auf Daten des Auftraggebers durch den Auftragnehmer werden protokolliert. Logging-Daten über administrative Zugriffe werden soweit möglich über einen Zeitraum von bis zu 180 Tagen vorgehalten und können im Bedarfsfall eingesehen werden.

3. Sicherstellung der Vertraulichkeit

Zutrittskontrolle

Maßnahmen
Der Zutritt zu den relevanten Technikräumen wird über Zutrittskontrollen bzw. -regelungen abgesichert. Hierzu existieren entsprechende organisatorische Anweisungen und elektronische Zutrittskontrollsysteme.
Der Serverraum ist fensterlos.
Es erfolgt eine 24-Stunden-Bewachung durch einen Schließdienst.
Die Schlüsselausgabe für Schlüssel zum Serverraum wird in einem Schlüsselbuch dokumentiert.
Die Räumlichkeiten mit Clientarbeitsplätzen sind mit einem Sicherheitsschließsystem ausgestattet.

Zugangskontrolle

Maßnahmen
Der Zugang zu den betroffenen Softwaresystemen wird generell nur über personalisierte Logins gewährt.
Zugangsberechtigungen zu Server, IT- und Softwaresystemen werden nur nach dem 4-Augenprinzip vergeben.
Die Anzahl der Personen mit administrativen Zugriffsmöglichkeiten auf Daten des Auftraggebers ist stets auf ein erforderliches Minimum reduziert.
Die Zugangsberechtigungen sind abgesichert mit zeitgemäßem Passwortschutz (Passwortregeln, u.a. Anzeige der Passwortqualität beim Festlegen eines neuen Passwortes, automatische Abmeldung nach 1 Stunde Inaktivität).
Der Betrieb der Server erfolgt in einer nach dem Stand der Technik abgesicherten Umgebung mit Firewall.
Die Passwörter aller Benutzer-Accounts werden ausschließlich als Hashwerte gespeichert und sind mit „Salt" und „Pepper" versehen.
Fernzugriffe sind nur über VPN-Technologie möglich.

Maßnahmen
Es kommt Antiviren Software zum Einsatz.
Soweit erforderlich sind Client Arbeitsplätze durch eine automatische passwortgesicherte Bildschirmsperre geschützt. Der Zugang zu den Datenverarbeitungssystemen wird protokolliert.
Anmelderechte ausgeschiedener Mitarbeiter werden sofort nach Beendigung des Arbeitsvertrags entzogen.

Zugriffskontrolle

Maßnahmen
Spezifische administrative Rechte werden durch ein dokumentiertes Rollenkonzept nachvollziehbar den jeweiligen Nutzern (Administratoren) zugeordnet.
Zugriff auf Daten des Auftraggebers haben nur Personen, die mit der Sicherstellung des ordnungsgemäßen und fehlerfreien Betriebs des Systems beauftragt sind.
Nicht mehr benötigte Datenträger werden durch Dienstleister vernichtet. Mit diesen Dienstleistern wurden die erforderlichen AV Verträge geschlossen.
Zugriffe auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten werden protokolliert.
Datenträger werden vor der Wiederverwendung physisch gelöscht.
Die Vernichtung von Datenträgern erfolgt gemäß der DIN 66399 (vormals 32757).
Die Anzahl von Administratoren ist auf das Notwendigste reduziert.
Datenträger werden sicher aufbewahrt.
Es existieren getrennte Test- und Produktivsysteme.

4. Sicherstellung von Nichtverkettbarkeit durch Zweckbestimmung

Verwendungszweckkontrolle/Trennungskontrolle

Maßnahmen
Das Anwendungssystem BLok ist umfassend mandantenfähig.
Es erfolgt eine technisch getrennte Datenverarbeitung mithilfe relationaler Datenbanken.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

Maßnahmen
Ein Datenschutzbeauftragter ist bestellt (siehe AV-Vertrag).
Verarbeitungsverzeichnisse werden regelmäßig überprüft und soweit notwendig aktualisiert.

Incident-Response-Management

Maßnahmen
Es ist ein IT-Sicherheitskonzept vorhanden.
Es sind entsprechende Notfallpläne vorhanden.

Datenschutzfreundliche Voreinstellungen

Maßnahmen
Es erfolgt eine auf notwendige Daten beschränkte Erhebung personenbezogener Daten.
Es besteht ein umfangreiches Rollen-Rechtekonzept für spezifische Nutzerzugänge.
Es besteht ein transparentes Betreuungskonzept.
Es ist ein Löschkonzept definiert.

Auftragskontrolle

Maßnahmen
Es erfolgen regelmäßige Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung.
Notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags werden vorgenommen.
Es besteht eine formalisierte Auftragserteilung.
Der Auftragnehmer hat schriftlich einen fachkundigen Datenschutzbeauftragten bestellt.
Die Mitarbeiter des Auftragnehmers werden soweit erforderlich mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut und in angemessenen Abständen entsprechend geschult bzw. sensibilisiert.

Anlage 2 - Subunternehmen

1. **BPS Bildungsportal Sachsen GmbH**

   Name und Anschrift:

   BPS Bildungsportal Sachsen GmbH
   Bahnhofstr. 6
   09111 Chemnitz

   Auftragsinhalt:

   Systembetrieb des Online-Berichtshefts BLok

2. **Technische Universität Chemnitz (Subunternehmen BPS GmbH)**

   Name und Anschrift:

   Technische Universität Chemnitz
   Universitätsrechenzentrum
   09107 Chemnitz

   Auftragsinhalt:

   Hosting des BLok-Servers (inkl. Backup)