Vereinbarung zur Auftragsverarbeitung gem. Art. 28 EU-DS-GVO

Zwischen

_____(Name der Schule)

_____(Straße)

_____(PLZ und Ort)

– nachstehend „Auftraggeber“ –

und der

Westermann Bildungsmedien Verlag GmbH

Georg-Westermann-Allee 66

38104 Braunschweig

– nachstehend „Auftragnehmer“ –

wird folgender Vertrag über Auftragsverarbeitung nach Art. 28 Abs. 3 und den weiteren Bestimmungen der Verordnung 2016/79 EU (EU Datenschutz-Grundverordnung) [i.F.: „EU-DS-GVO“], sowie sonstiger anwendbarer datenschutzrechtlicher Bestimmungen geschlossen:

§ 1 Gegenstand und Dauer des Auftrags, Auftragsinhalt

1. **Inhalt**
   Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag der Auftraggeberin. Inhalt des Vertrages ist die Regelung aller datenschutzrechtlicher Fragen zwischen Auftraggeberin und Auftragnehmerin.

2. **Gegenstand des Auftrags**
   Der Gegenstand des Auftrags ergibt sich aus der in Anlage 1 beschriebenen Leistungsvereinbarung (im Folgenden „Leistungsvereinbarung“).

3. **Dauer des Auftrags**
   Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

4. **Art und Zweck der vorgesehenen Verarbeitung von Daten**
   Art und Zweck der Verarbeitung personenbezogener Daten durch die Auftragnehmerin für die Auftraggeberin sind in der Leistungsvereinbarung konkret beschrieben.

5. **Ort der Datenverarbeitung**
   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 Information der Auftraggeberin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DS-GVO erfüllt sind.

6. **Art der Daten**
   Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben.

7. **Kategorien betroffener Personen**

   Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben.

§ 2 Pflichten / Kontrollrecht des Auftraggebers

1. Der Auftraggeber ist alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchzuführenden Verarbeitung durch den Auftragnehmer im Hinblick auf die Regelungen der EU Datenschutz-Grundverordnung und anderer Vorschriften über den Datenschutz.

2. 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 rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

   Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-DS-GVO 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.

   Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z.B. auch erfolgen durch:

   - Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DS-GVO
   - Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DS-GVO
   - 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, ISO 27001).

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

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Ein Datenschutzbeauftragter ist beim Auftragnehmer bestellt worden. Er kann unter der E-Mail Adresse datenschutzbeauftragter@westermanngruppe.de kontaktiert werden.

2. Die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DS-GVO wird gewahrt. 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. Diese gelten auch nach Beendigung des Auftrags fort.

3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DS-GVO [Einzelheiten in Anlage 2].

4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. 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 Personen gewährleistet wird.

6. Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im Rahmen der vertraglich festgelegten Weisungen und der speziellen Einzelweisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (beispielsweise bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt.

   Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
   Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Weisungsberechtigten beim Auftraggeber bestätigt oder geändert wird.

7. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Unterlagen und Daten betroffen sind.

8. Der Auftragnehmer führt das Verzeichnis der Verarbeitungstätigkeit gem. Art. 30 Abs. 2 EU-DS-GVO und stellt dies auf Anfrage dem Auftraggeber zur Verfügung. Der Auftraggeber stellt dem Auftragnehmer die hierzu erforderlichen Informationen zur Verfügung.
   Der Auftragnehmer unterstützt den Auftraggeber seinerseits bei der Erstellung des Verzeichnisses nach Art 30 Abs. 1 EU-DS-GVO.

9. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten.

10. Der Auftragnehmer informiert den Auftraggeber unverzüglich 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.

    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.

11. Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes (z. B. technischer Art), im Falle einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (Art. 33 Abs.2 EU-DS-GVO).

12. Die Datenverarbeitung findet grundsätzlich in den Betriebsstätten der Auftragnehmerin statt. Soweit die Verarbeitung von Daten in Privatwohnungen durch vorher festgelegte Nutzungsberechtigte erforderlich wird, stellt die Auftragnehmerin sicher, dass diese Verarbeitung ausschließlich auf Dienstgeräten der Auftragnehmerin erfolgt und technisch und organisatorisch dem jeweiligen Stand der Technik entspricht. Fernzugriffe erfolgen ausschließlich auf Firmenserver der Auftragnehmerin über gesicherter VPN-Verbindungen und Passwortabfragen. Darüber hinaus stellt die Auftragnehmerin sicher, dass die Personen, die diese Datenverarbeitung in ihrer Privatwohnung durchführt, organisatorisch über den Umgang und die Verarbeitung von personenbezogenen Daten belehrt wurde. Die in Anlage 2 geregelten Maßnahmen nach Art. 32 EU-DS-GVO sind auch in diesem Fall sicherzustellen.

§ 4 Rückgabe und Löschung

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 Kopien, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind.

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.

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.

§ 5 Unterauftragsverhältnisse

1. Der Auftragnehmer darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.

   Der Auftraggeber stimmt der Beauftragung der in Anlage 3 aufgeführten Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4, 9 EU-DS-GVO, welche sowohl schriftlich als auch in einem elektronischen Format erfolgen kann.

2. Vor Hinzuziehung weiterer oder Ersetzung aufgeführter Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber eine angemessene Zeit vorab schriftlich oder in

Textform.

3. Der Auftraggeber kann gegen die Änderung – innerhalb einer angemessenen Frist, jedoch nicht länger als 2 Wochen – aus wichtigem datenschutzrechtlichem Grund – gegenüber der vom Auftragnehmer bezeichneten Stelle Einspruch erheben. Erfolgt kein Einspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Bei unberechtigtem Einspruch kann es zu entsprechenden Verzögerungen bei der Erbringung der Leistung nach dem Hauptvertrag kommen. Für eine aus einem unberechtigten Einspruch resultierende Einschränkung der Vertragsleistungen ist der Auftragnehmer nicht verantwortlich.

   Hat der Auftraggeber aufgrund eines wichtigen datenschutzrechtlichen Grundes berechtigt Einspruch gegen einen Unterauftragsverarbeiter erhoben und ist eine einvernehmliche Lösungsfindung zwischen den Parteien auch auf anderem Wege aufgrund von wichtigen datenschutzrechtlichen Gründen nicht möglich, steht dem Auftragnehmer ein Sonderkündigungsrecht zu.

   In Ausnahmefällen ist auch eine nachträgliche Einigung zwischen den Parteien möglich. Der Auftragnehmer hat den Auftraggeber in diesem Fall unverzüglich über den Einsatz eines Unterauftragsverarbeiters zu informieren.

4. Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU / des EWR, stellen Auftraggeber und Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

5. Eine weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mindestens Textform); sämtliche vertragliche Regelungen zu den Datenschutzpflichten in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.

6. 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 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.

§ 6 Weisungsrechte

Der Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber erteilt alle Weisungen und Aufträge in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und in schriftlicher oder elektronischer Form zu dokumentieren.

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format.

- Weisungsberechtigt bei der Auftraggeberin ist die Schulleitung, die weitere Weisungsberechtigte benennen kann.

- Weisungsempfänger bei der Auftragnehmerin sind die Mitarbeiterinnen und Mitarbeiter der Kundenbetreuung der Auftragnehmerin.

  Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

  Weisungen der Auftraggeberin an die Auftragnehmerin werden ausschließlich von den o.g. verantwortlichen Sachgebietsbearbeitern erteilt.

§ 7 Rechte betroffener Personen

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. Dem Auftraggeber obliegen die aus den Artikeln 15 bis 21 EU-DSGVO resultierenden Pflichten gegenüber den Betroffenen, insbesondere über Auskunft, Berichtigung und Löschung. Der Auftragsverarbeiter wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III EU-DSGVO genannten Rechte der betroffenen Person nachzukommen.

§ 8 Technisch-organisatorische Maßnahmen

1. Die in der Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.

   Der Auftragnehmer hat damit die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-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 EU-DS-GVO zu berücksichtigen.

2. 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.

3. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder

Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

§ 9 Haftung

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder dieser Datenschutzvereinbarung gelten die gesetzlichen Vorschriften, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

§ 10 Sonstiges

1. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung 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.

2. Der Gerichtsstand für beide Parteien ist Braunschweig.

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

……, den ……

Für den Auftraggeber:

Name Unterschrift

Für den Auftragnehmer:

Name Unterschrift

Anlage 1: Leistungsvereinbarung

Gegenstand des Auftrages:

Bereitstellung und Betrieb folgender Lernplattformen durch den Auftragnehmer während der Dauer ihrer jeweiligen Lizenzierung durch den Auftraggeber.

	Einsatzzweck der Anwendung
Online-Diagnose	Die Online-Diagnose dient der individuellen Förderung von Schüler/-innen in den Fächern Deutsch, Mathematik und Englisch für die Klassenstufen 5 bis 9 basierend auf einer Lernstandserhebung in den wichtigsten Kompetenzbereichen eines Jahrgangs. Zu diesem Zweck stellt die Anwendung der Lehrkraft Auswertungen der Schüler/-innen in den getesteten Kompetenzbereichen zur Verfügung. Die Schüler/-innen erhalten individuell angepasste Fördermaterialien
kapiert.de für die Schule	kapiert.de für die Schule dient der unterrichtsbegleitenden, individuellen Förderung von Schülerinnen und Schülern in Mathematik, Deutsch und Englisch in der Sekundarstufe I mit Hilfe von ergänzenden, digitalen Erkläreinheiten, Übungen und Tests.
BiBox / Interaktive Übungen	Die BiBox und die interaktive Übungen dienen dem Erwerb der im jeweiligen Lehrplan für die Klassenstufe vorgegebenen fachspezifischen Kompetenzen basierend auf der Arbeit mit dem digitalen Schulbuch und zusätzlichen multimedialen Lern- und Lehrinhalten sowohl im Unterricht als auch beim Lernen und Üben zu Hause.

Art und Zweck der vorgesehenen Verarbeitung:

Für die Schüler/-innen wird in der jeweiligen Lernplattform ein Account eingerichtet, mit dem sie im jeweiligen System arbeiten können.

Art der Daten:

Datum	**Begründung der Verarbeitung**
Identifier der Schüler/-in (Vorname, Name – es können auch Fantasienamen genutzt werden)	Identifizierung des Schülers / der Schülerin in Auswertungen für die Lehrkraft
Benutzername / Kennwort (Account)	Steuerung des Zugriffs zur Lernplattform
Geschlecht	Erzeugung von Texten
Klassenstufe/-bezeichnung	Definition einer Organisationeinheit für die Schüler/-innen im System
Nur Online Diagnose / kapiert.de	
bearbeitete Fragen/Aufgaben mit automatischer Auswertung (richtig / falsch)	Basis der im System für die Lehrkraft erzeugten Übersichten
Bearbeitungsdauer und -Zeitpunkt	Basis der im System für die Lehrkraft erzeugten Übersichten
Nur BiBox / Interaktive Übungen	
Lesezeichen, Annotationen, Notizen, eigene Dateien der Schülerin / des Schülers	Ermöglicht die individuelle Arbeit der Schüler/in mit dem digitalen Schulbuch
von der Lehrkraft der Schüler/-in zugeordnete Dateien	Ermöglicht den individuellen Lehrwerkeinsatz durch die Lehrkraft

Kategorien betroffener Personen:

Schüler/-innen der datenverarbeitenden Stelle, die in der Anwendung eingerichtet werden.

Anlage 2: Allgemeine technische und organisatorische Maßnahmen

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

a) Zutrittskontrolle

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

Die Server sind in einem Sicherheitsbereich untergebracht, der überwacht ist und zu dem nur befugte Personen Zugriff haben. Dabei wird die Anwesenheit aufgezeichnet. Die Zugangskontrolle erfolgt über eine gesondert freigeschaltete Codekarte. Besucher dürfen sich nur in Begleitung eines Mitarbeiters im Sicherheitsbereich aufhalten. Eine Einbruchsmeldeanlage wird eingesetzt.

Datensicherungen auf Datenträgern werden in einem vom Serverbetrieb getrennten gesicherten Bereich des Rechenzentrums vorgehalten. Zugang zu den Datenträger zur Sicherung hat nur hierfür befugtes Personal des Rechenzentrums.

---

b) Zugangskontrolle

Eine unbefugte Systemnutzung ist zu verhindern.

Der Netzwerkzugang zu den Anwendungen im Backend ist durch eine zweistufige Firewall Technologie geschützt. Zum einen über einen dedizierten Firewall Rechner für das über Internet erreichbare Teilnetz des Auftragnehmers und darüber hinaus über IP-Filter direkt auf dem jeweiligen Applikationsserver. Ein dediziertes System zur Intrusion Detection wird eingesetzt. Administrative Zugänge auf den Anwendungsserver, den Datenbankserver und weitere administrative Systeme (z.B. Lizenzverwaltung) haben nur die unmittelbar mit der Systempflege beschäftigten Mitarbeiter des Rechenzentrums sowie die Internet-Administratoren des Auftragnehmers. Der Zugriff auf Systemebene ist nur aus dem Intranet und dem Netz des Rechenzentrums möglich, sowie über eine zertifikatsbasierte, personalisierte VPN-Verbindung. Die Zertifikate haben eine Gültigkeit von 1 Jahr. Das Betriebssystem und die Softwarekomponenten der Anwendung werden regelmäßig und zeitnah unter besonderer Berücksichtigung von Sicherheitsaspekten aktualisiert. Die Administratoren authentifizieren sich lokal oder über einen zentralen Authentifizierungsserver. Ein Login auf den Servern selbst ist nur per SSH möglich. Die Passwörter für die Authentifizierung erfüllen die Voraussetzungen des BSI- Grundschutzes. Sie müssen regelmäßig geändert werden, der Änderungszeitraum ist softwaremäßig vorgegeben.

---

c) Zugriffskontrolle / Benutzerkontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.

Der Zugriff auf Daten und Dienste der Anwendung wird über eine differenzierte Zugriffsregelung, basierend auf Gruppen geregelt.

Die Berechtigungsvergabe erfolgt im Rahmen eines protokollierten Workflow-Prozesses.

Die Authentifikation gegenüber der Anwendung erfolgt mit Benutzername / Passwort unter Verwendung von individualisierten Accounts.

Die Änderung von Daten wird protokolliert.

---

d) Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

Für das Testen der Anwendung stehen Testsysteme zur Verfügung, die vom Produktivsystem getrennt sind. Es werden keine personenbezogenen Daten von Nutzern in Testsystemen eingesetzt.

Support-Systeme sind vom Produktivsystem der Auftragsverarbeitung getrennt.

Berechtigungen werden auf Anwendungsebene vergeben.

---

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DS-GVO, Art. 25 Abs. 1 EU-DS-GVO)

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Die in der Anwendung verarbeiteten personenbezogenen Daten sind nach dem Prinzip der Datensparsamkeit auf das notwendige Minimum reduziert.

Sofern die Verarbeitung auch anonym erfolgen kann, wird auf den Personenbezug verzichtet.

Soweit technisch umsetzbar, wird zusätzlich eine Verschlüsselung für die Übermittlung und Speicherung eingesetzt

---

---

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

a) Weitergabekontrolle / Übertragungskontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

Daten werden bei elektronischer Übertragung verschlüsselt übertragen. Übertragungen werden entsprechend protokolliert. Werden Daten auf Weisung des Aufraggebers an Dritte übermittelt, so hat die Aufforderung schriftlich zu erfolgen und wird in einer Übersicht erfasst.

Datenträger werden nur zu Backup Zwecken genutzt und nicht zum Transport von Daten. Datenträger sind im Rechenzentrum gegen unbefugtes Entfernen geschützt und regelmäßige Bestandskontrollen finden statt. Die Vernichtung von Datenträgern findet kontrolliert mit Protokollierung statt.

---

b) Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Anwendung loggt das Anlegen, Ändern und Löschen personenbezogener Daten mit.

Die entsprechenden Rechte werden auf Basis des Berechtigungskonzeptes aufgrund von Berechtigungsanfragen über einen Workflow-Prozess vergeben.

---

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

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

Es werden unterbrechungsfreie Stromversorgung, Dieselgeneratoren und Klimaanlagen eingesetzt. Das Rechenzentrum verfügt über Schutzmaßnahmen im Brandfall.

Um die Gefahr des Datenverlustes zu minimieren werden RAID Systeme auf den Servern eingesetzt.

Eine tägliche Datensicherung der System- und Anwendungsdaten auf physischen Datenträgern wird vorgenommen (Sicherheits-Backup).

---

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

a) Datenschutz-Management

b) Incident-Response-Management

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

d) Auftragskontrolle

Der Datenschutzbeauftragte ist benannt. Verantwortliche für Datensicherheit, Auftragskontrolle und aktuelle Dokumentation der Verfahrensschritte sind definiert.

Die mit der Anwendung befassten Mitarbeiter/innen haben klar definierte Aufgaben und sind auf das Datengeheimnis verpflichtet.

Die interne Organisation ist so gestaltet, dass Weisungen des Auftraggebers schriftlich zu erfolgen haben und die zeitnahe und auftragskonforme Durchführung der Anweisung kontrolliert werden kann.

Datenschutz und Datensicherheit sind elementare Bestandteile von Softwareverträgen.

Jede Hardware und Software durchläuft im Rahmen der Investitionsplanung ein Genehmigungsverfahren. Software und Änderungen sind dokumentiert.

Für jede eingesetzte Software sind die Zugriffsrechte geregelt und dokumentiert.

Eingesetzte Software wird mit Updates aktuell gehalten.

Anlage 3: Unterauftragsverarbeiter des Auftragnehmers

Name und Adresse von Unterauftragsverarbeiter 1	**Durchzuführende Tätigkeit(en)**
Name: Westermann Service und Beratung GmbH Geschäftsführerin: Nicole Bornemann Strasse / Postfach: Georg-Westermann-Allee 66 PLZ Ort: 38104 Braunschweig Die datenschutzrechtlichen Voraussetzungen dieser Vereinbarung werden entsprechend im Vertragsverhältnis mit dem Unterauftragsverarbeiter eingehalten.	Kundenberatung per E-Mail und Telefon
Name und Adresse von Unterauftragsverarbeiter 2	**Durchzuführende Tätigkeit(en)**
Name: Westermann GmbH & Co. KG Geschäftsführer: Sven Fischer (CEO), Timo Blümer (CFO) Straße / Postfach: Georg-Westermann-Allee 66 PLZ Ort: 38104 Braunschweig Die datenschutzrechtlichen Voraussetzungen dieser Vereinbarung werden entsprechend im Vertragsverhältnis mit dem Unterauftragsverarbeiter eingehalten.	Technische Betreuung der Anwendung
Name und Adresse von Unterauftragsverarbeiter 3	**Durchzuführende Tätigkeit(en)**
Name: Gärtner Datensysteme GmbH & Co. KG Geschäftsführer: Christine Müller, Martin Neitzel, Ulrich Schwarz, Stefan Gärtner Strasse / Postfach: Hamburger Straße 273 a PLZ Ort: 38144 Braunschweig Die datenschutzrechtlichen Voraussetzungen dieser Vereinbarung werden entsprechend im Vertragsverhältnis mit dem Unterauftragsverarbeiter eingehalten.	Rechenzentrumsbetrieb

Die Zustimmung zum Einsatz des/der oben genannten Unterauftragsverarbeiters/Unterauftragsverarbeiter für die genannten durchzuführenden Tätigkeiten werden erteilt, sofern die datenschutzrechtlichen Voraussetzungen entsprechend dieser Vereinbarung auch in diesem Vertragsverhältnis (Unterauftragsverarbeiter-ADV) eingehalten werden.