Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO

zwischen

Land Baden-Württemberg
vertreten durch das
Ministerium für Kultus, Jugend und Sport,
vertreten durch das
Institut für Bildungsanalysen Baden-Württemberg (IBBW)
vertreten durch den Direktor Dr. Günter Klein

– nachfolgend „**Auftraggeber“** genannt –

und

Westermann Bildungsmedien Verlag GmbH
Georg-Westermann-Allee 66
38104 Braunschweig
als Auftragsverarbeiter
– nachfolgend **„Auftragnehmer“** genannt –

Auftraggeber und Auftragnehmer jeweils auch als „**Partei**“ und zusammen als „**Parteien**“ bezeichnet.

Präambel

Der Auftraggeber hat den Auftragnehmer mit Leistungen im Bereich der Bereitstellung eines digitalen, wissenschaftlich basierten, diagnostischen Instruments zur Beurteilung der Englischkompetenzen an weiterführenden öffentlichen Schulen in Baden-Württemberg beauftragt. Die Leistungen werden von der jeweiligen öffentlichen Schule (nachfolgend **„Abrufberechtigte“**) bei dem Auftragnehmer abgerufen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 Datenschutzgrundverordnung (DSGVO) gilt in diesem Zusammenhang nicht der Auftraggeber, sondern die jeweilige Abrufberechtigte.

Im Verhältnis zwischen den Parteien soll diese Vereinbarung ein ausreichendes Datenschutzniveau bei der Ausführung der durch den Auftraggeber beauftragten Leistungen sicherstellen. Die Abrufberechtigten können dieser Vereinbarung durch einseitige Erklärung beitreten.

Im Verhältnis zwischen Auftragnehmer und der jeweiligen Abrufberechtigten konkretisiert diese Vereinbarung die datenschutzrechtlichen Rechte und Pflichten gemäß Art. 28 Abs. 3 Datenschutzgrundverordnung (DSGVO) im Zusammenhang mit dem Umgang des Auftragnehmers oder von ihm unterbeauftragte Dritte mit personenbezogenen Daten zur Durchführung des Hauptvertrages. Die Erfüllung der Auftragsverarbeitungsvereinbarung wird nicht gesondert vergütet.

Es werden die Begriffsdefinitionen der DSGVO zugrunde gelegt.

Inhaltsverzeichnis

1. Vertragsparteien

1.1 Der Auftraggeber schließt diese Vereinbarung, um ein angemessenes Datenschutzniveau bei dem von dem Auftraggeber beauftragten Leistungen sicherzustellen. Der Auftraggeber selbst ist nicht Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

1.2 Die Parteien sind sich einig, dass die jeweiligen Abrufberechtigten dieser Vereinbarung durch einseitige Erklärung in schriftlicher oder Textform als eigenständige Verantwortliche im Sinne des Art 4 Nr. 7 DSGVO beitreten können. Die Abrufberechtigte erklärt den Beitritt gegenüber dem Auftragnehmer. Der Beitritt durch die jeweilige Abrufberechtigte bedarf keiner Annahme durch die Parteien.

1.3 Eine gemeinsame Verantwortlichkeit der Abrufberechtigten wird nicht begründet. Durch Beitritt zu dieser Vereinbarung ist jede Abrufberechtigte für die Verarbeitung der in ihrer Verantwortlichkeit liegenden personenbezogenen Daten eigenständig verantwortlich.

1.4 Der Auftragnehmer ist Auftragsverarbeiter im Sinne des Art. 28 DSGVO.

2. Vertragsgegenstand und Dauer

2.1 Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Bereitstellung eines digitalen, wissenschaftlich basierten, diagnostischen Instruments zur Beurteilung der Englischkompetenzen an weiterführenden öffentlichen Schulen in

Baden-Württemberg auf Grundlage der Rahmenvereinbarung über die Bereitstellung von Diagnoseinstrumenten vom 21.08.2023 („Hauptvertrag“).

Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung der Abrufberechtigten, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus Anlage 1 sowie dem Hauptvertrag (und sofern vorhanden aus der dazugehörigen Leistungsbeschreibung). Der Abrufberechtigten obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

2.2 Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

2.3 Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die von der Abrufberechtigten stammen oder für die Abrufberechtigte erhoben wurden oder auf sonstige Weise in deren Auftrag verarbeitet (nachfolgend „**Abrufberechtigten-Daten**“ genannt) werden.

2.4 Die Abrufberechtigten-Daten werden vom Auftragnehmer nur für die Anlage 1 angegebene Dauer verarbeitet.

2.5 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung der Abrufberechtigten in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten sowie Kategorien der von der Verarbeitung betroffenen Personen und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anlage 1 aufgeführt. Im Übrigen ergeben sich Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer aus dem Hauptvertrag (und sofern vorhanden aus der dazugehörigen Leistungsbeschreibung).

4. Weisungsrecht

4.1 Der Auftragnehmer darf Abrufberechtigten-Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen der Abrufberechtigten erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er der Abrufberechtigten diese rechtlichen Anforderungen vor der Verarbeitung mit.

4.2 Die Weisungen der Abrufberechtigten werden anfänglich durch diesen Vertrag festgelegt und können von der Abrufberechtigten danach in schriftlicher Form oder in dokumentiertem elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Abrufberechtigte ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. In Abstimmung mit dem Abrufberechtigten ist der Auftraggeber berechtigt, Weisungen gegenüber dem Auftragnehmer zu erteilen. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen sind:

Anrede, Vorname, Nachname	Kontaktdaten
Frau Maren Specker (IBBW)	E-Mail: maren.specker@ibbw.kv.bwl.de Tel: 0711 6642-4102
Herr Dr. Stephan Blank (IBBW)	E-Mail: stephan.blank@ibbw.kv.bwl.de Tel: 0711 6642-4100

Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen

4.3 Alle erteilten Weisungen sind sowohl von der Abrufberechtigten als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

4.4 Ist der Auftragnehmer der Ansicht, dass eine Weisung der Abrufberechtigten gegen datenschutzrechtliche Bestimmungen verstößt, hat er die Abrufberechtigte

unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch die Abrufberechtigte bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

5.2 Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter bestellt:

Norbert, Rauch, norbert.rauch@atrarax.de; 09132 – 79800
Vorname, Name, E-Mail (Funktionspostfach), Telefonnr.

5.3 Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend „**eingesetzte Personen**“ genannt), entsprechend zur Vertraulichkeit verpflichten, es sei denn sie unterliegen bereits einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Den bei der Datenverarbeitung durch den Auftragnehmer eingesetzten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Der Abrufberechtigten sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

5.4 Die Verarbeitung von Abrufberechtigten-Daten, die Gegenstand dieser Vereinbarung sind, in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur gestattet, sofern die Einhaltung Verpflichtungen dieser Vereinbarung sowie der Maßgaben des Art. 32 DS-GVO auch in diesem Fall sichergestellt sind. Der Auftragnehmer hat die Abrufberechtigte über die Verarbeitung von Abrufberechtigten-Daten in Privatwohnungen sowie die getroffenen Sicherheitsmaßnahmen in Textform zu unterrichten.

5.5 Der Auftragnehmer wird die Abrufberechtigte unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen

durch geeignete technische und organisatorische Maßnahmen bei der Einhaltung der in Art. 32-36 DS-GVO genannten Pflichten unterstützen, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgeabschätzung und der Konsultation mit Aufsichtsbehörden.

5.6 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer die Abrufberechtigte unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Der Auftragnehmer ist verpflichtet den vorstehenden Informationspflichten nachzukommen, soweit die Vorfälle und Prüfungen Auswirkungen auf die datenschutzkonforme Verarbeitung von Auftraggeber-Daten haben könnten. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber die Abrufberechtigte und ersucht diese um weitere Weisungen. Der Auftragnehmer ist darüber hinaus verpflichtet, der Abrufberechtigten jederzeit Auskünfte zu erteilen, soweit deren Daten von einer Verletzung nach Absatz 1 betroffen sind. Meldungen für die Abrufberechtigte nach Art. 33 oder 34 DSGVO darf der Auftragnehmer nur nach vorheriger Weisung seitens der Abrufberechtigten gem. Ziffer 3 dieser Vereinbarung durchführen.

5.7 Sollten die Daten der Abrufberechtigten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer die Abrufberechtigte unverzüglich darüber zu informieren, sofern ihm dies nicht durch

gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich bei der Abrufberechtigten als „Verantwortlichen“ im Sinne der DSGVO liegen.

5.8 Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist der Abrufberechtigten unverzüglich in Textform mitzuteilen.

5.9 Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag der Abrufberechtigten durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist der Abrufberechtigten auf Anforderung zur Verfügung zu stellen. Der Auftragnehmer wird der Abrufberechtigte die für die Führung des Verzeichnisses der Verarbeitungstätigkeiten notwendigen Informationen zur Verfügung stellen.

6. Technische und organisatorische Sicherheitsmaßnahmen

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten der Abrufberechtigten gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 2 ergänzten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Der Auftragnehmer legt auf Anforderung der Abrufberechtigten die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Sämtliche Anpassungen sind vom Auftragnehmer zu dokumentieren und der Abrufberechtigten regelmäßig (mindestens jährlich) schriftlich oder in Textform mitzuteilen. Die Abrufberechtigte kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern. Über wesentliche Änderungen der Sicherheitsmaßnahmen hat der Auftragnehmer die Abrufberechtigte unverzüglich in Textform zu unterrichten.

7. Kontrollrechte der Abrufberechtigten

7.1 Die Abrufberechtigte überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der in diesem Vertrag niedergelegten Pflichten durch den Auftragnehmer, insbesondere der technischen und organisatorischen

Maßnahmen. Hierfür kann er vom Auftragnehmer alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten verlangen, z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers in der Regel nach rechtzeitiger Anmeldung, sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint, zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Die Abrufberechtigte wird darauf achten, dass die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig gestört werden.

7.2 Der Auftragnehmer verpflichtet sich, der Abrufberechtigten auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der Einhaltung der in diesem Vertrag niedergelegten Pflichten sowie der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind und Vor-Ort-Kontrollen zuzulassen. Bei mündlichen Anforderungen ist der Auftragnehmer berechtigt eine Bestätigung der Anforderung in Textform zu verlangen.

7.3 Die Abrufberechtigte dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die die Abrufberechtigte insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat sie den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt die Abrufberechtigte dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

7.4 Der Auftragnehmer stellt der Abrufberechtigten auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

7.5 Der Auftragnehmer weist der Abrufberechtigten die Verpflichtung der Mitarbeiter nach Ziffer 4.3 auf Verlangen nach.

7.6 Die Abrufberechtigte lässt die Kontrolle gemäß Ziff. 7.1 und 7.3 in der Regel von dem Auftraggeber durchführen, welcher die Kontrolle dokumentiert und die Abrufberechtigte über das Ergebnis der Kontrolle informiert. Der Auftragnehmer verpflichtet sich die Verpflichtungen aus Ziff. 7.1 bis 7.5 auch gegenüber dem Auftraggeber zu erbringen. Der Abrufberechtigten bleibt es unbenommen eigene Kontrollen durchzuführen.

8. Einsatz von Subunternehmern

8.1 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 3 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er die Abrufberechtigte hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich oder in dokumentiertem elektronischen Format zugestimmt hat. In Abstimmung mit den Abrufberechtigten ist der Auftraggeber berechtigt die Zustimmung der Abrufberechtigten einzuholen und gegenüber dem Auftragnehmer zu erteilen. Eine Verpflichtung des Auftraggebers soll damit nicht begründet werden. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten, indem er diesem dieselben Datenschutzpflichten auferlegt und dabei sicherzustellen, dass die Abrufberechtigte ihre Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, bedarf dies der gesonderten Zustimmung der Abrufberechtigten und der Auftragnehmer hat sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird der Abrufberechtigten auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

8.2 Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung der Abrufberechtigten. In Abstimmung mit den Abrufberechtigten ist der Auftraggeber berechtigt die Zustimmung der Abrufberechtigten einzuholen und gegenüber dem Auftragnehmer zu erteilen. Eine Verpflichtung des Auftraggebers soll damit nicht begründet werden.

8.3 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für die Abrufberechtigte erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die

auch im Zusammenhang mit der Erbringung von Leistungen für die Abrufberechtigte genutzt werden.

9. Anfragen und Rechte betroffener Personen

Der Auftragnehmer wird angesichts der Art der Verarbeitung die Abrufberechtigte nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Betroffenenrechte unterstützen. Sollte sich ein Betroffener direkt an den Auftragnehmer wenden, um die Betroffenenrechte erkennbar hinsichtlich der im Auftrag der Abrufberechtigten verarbeiteten Abrufberechtigten-Daten wahrzunehmen, wird der Auftragnehmer dieses Ersuchen unverzüglich an die Abrufberechtigte weiterleiten und dessen Weisung abwarten.

10. Haftung

10.1 Die Haftung der Parteien und der Abrufberechtigten richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber der Abrufberechtigten oder dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

10.2 Die Parteien sowie die Abrufberechtigte stellen sich jeweils von der Haftung frei, wenn eine Partei oder die Abrufberechtigte nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

11. Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer gegen seine Pflichten aus diesem Vertrag schwerwiegend verstößt, Bestimmungen der DSGVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung der Abrufberechtigten nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten der Abrufberechtigten auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

12. Beendigung des Hauptvertrags

12.1 Der Auftragnehmer wird der Abrufberechtigten nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Abrufberechtigten-Daten und Datenträger zurückgeben oder – auf Wunsch des der

Abrufberechtigten, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Abrufberechtigten-Daten zu führen.

12.2 Die Abrufberechtigte hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Abrufberechtigten-Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

12.3 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Abrufberechtigten-Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm von der Abrufberechtigten zugeleitet wurden oder die er für diese erhoben hat.

13. Schlussbestimmungen

13.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

13.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

13.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

13.4 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Stuttgart.

Folgende Dokumente sind untrennbarer Bestandteil dieser Vereinbarung:

Anlage 1 Beschreibung der Verarbeitung

Anlage 2 Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Anlage 3 Unterauftragsverhältnisse beim Auftragnehmer

Auftraggeber	**Auftragnehmer**
Stuttgart, 26.10.2023	Braunschweig, 23.10.2023
(Ort/Datum)	(Ort/Datum)
Dr. Stephan Blank, i.A. der Direktion	Frank Tscherwen, Geschäftsführer

Anlage 1

Beschreibung der Verarbeitung

I. Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist ein wissenschaftlich basiertes, diagnostisches Instrument speziell zur Beurteilung der Englischkompetenzen (Lese- und Hörverständnis, Sprachliche Mittel) von Schülerinnen und Schülern der weiterführenden öffentlichen Schulen in Baden-Württemberg, welches lehrplanunabhängig den allgemeinen Leistungsstand der schulischen und alltäglichen Englischkenntnisse misst

II. Dauer der Verarbeitung

Die Verarbeitung beginnt mit Einzelabruf und endet spätestens mit Erfüllung des letzten auf Basis des Hauptvertrages abgerufenen Einzelauftrages.

III. Art der Verarbeitung

Erfassung, Speicherung sowie systeminterne Auswertung im Rahmen der Stärken-Schwächen-Bewertung sowie der Zusammenstellung passender Fördermaterialien.
(In welcher Form erfolgt die Verarbeitung? Erfassen, Speichern, Auslesen, Anpassen etc.)

IV. Zweck der Verarbeitung

Bereitstellung eines wissenschaftlich basierten, diagnostischen Instruments zur Beurteilung der Englischkompetenzen von Schülern. Im Übrigen richtet sich der Zweck der Vereinbarung nach dem Hauptvertrag

V. Art der personenbezogenen Daten

☒	**Personenstammdaten**	Vor- und Nachname, Titel, Anrede, Geschlecht, Geburtsort, Geburtsdatum
☒	**Adressdaten**	Anschrift, Ort, Straße, Postleitzahl
☒	**Kontaktdaten**	E-Mail-Adresse, Telefonnummer, Faxnummer
☒	**Profildaten**	Eintragungen bei Tests, Auswertungen der Testergebnisse, empfohlene Fördermaterialien
☐	_____	

VI. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

☒ **Schüler**
☒ **Lehrkräfte**
☒ **Abrufberechtigte** **inkl. Beschäftigte der Abrufberechtigten**
☐ _____

Anlage 2

Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

---

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 dem 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

Unterauftragsverhältnisse beim Auftragnehmer

Unterauftragnehmer (Firmenname mit Rechtsform)	**Beschreibung der (Teil-)Leistungen**	**Anschrift/ Ort der Leistungserbringung**	**Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO**
Westermann Service und Beratung GmbH	Kundenberatung per E-Mail und Telefon	Georg-Westermann-Allee 66, 38104 Braunschweig	Insoweit gelten die vom Auftragnehmer auf entsprechende Nachforderung vom 26.07.2023 am 01.08.2023 im vorgelagerten Vergabeverfahren nachgereichten Angaben („Anlage B - Darstellung der Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO“)
Westermann GmbH & Co. KG	Technische Betreuung der Anwendung	Georg-Westermann-Allee 66, 38104 Braunschweig	Insoweit gelten die vom Auftragnehmer auf entsprechende Nachforderung vom 26.07.2023 am 01.08.2023 im vorgelagerten Vergabeverfahren nachgereichten Angaben („Anlage B - Darstellung der Maßnahmen zur Gewährleistung eines angemessenen

Unterauftragnehmer (Firmenname mit Rechtsform)	**Beschreibung der (Teil-)Leistungen**	**Anschrift/ Ort der Leistungserbringung**	**Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO**
			Schutzniveaus gem. Art. 44 ff. DSGVO“)
Gärtner Datensysteme GmbH und Co. KG	Rechenzentrumsbetrieb und technische Entwicklung der Anwendung	Hamburger Straße 273 a, 38144 Braunschweig	Insoweit gelten die vom Auftragnehmer auf entsprechende Nachforderung vom 26.07.2023 am 01.08.2023 im vorgelagerten Vergabeverfahren nachgereichten Angaben („Anlage B - Darstellung der Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO“)

Anlage B - Darstellung der Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO

Anlage B - Darstellung der Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO

Unterauftragnehmer (Firmenname mit Rechtsform)	**Beschreibung der (Teil-)Leistungen**	**Anschrift/ Ort der Leistungserbringung**	**Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO***
Westermann Service und Beratung GmbH	Kundenberatung per E-Mail und Telefon	Georg-Westermann-Allee 66, 38104 Braunschweig	**1. Zutrittskontrolle** Der Unterauftragnehmer stellt sicher, dass Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen haben. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Sicherheitsschlösser mit Schlüsselregelung • verschlossene Türen bei Abwesenheit • Fenstersicherung (insbesondere im Erdgeschoss) • Festlegung von Sicherheitsbereichen • Zutrittskontrollsystem mit Chipkarte sowie ergänzend kontrollierte Schlüsselvergabe • Schließsystem inkl. zeitabhängiger Berechtigungen • Protokollierung der Zu- und Abgänge • Zutrittsregelungen für betriebsfremde Personen inkl. Besucherausweis • Empfang mit Werkschutz und Pförtner • Überwachungseinrichtungen der IT Räume mit Alarmanlage

			• Videoüberwachung **2. Zugangskontrolle** Der Unterauftragnehmer stellt sicher, dass Unbefugt keinen Zugang zu den Datenverarbeitungssystemen haben. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Persönlicher User-Account für die Anmeldung an das Unternehmensnetz und die Systeme • Autorisierungsprozess für die Vergabe von Zugriffsberechtigungen • Regelbasiertes Löschen ausgeschiedener Mitarbeiter • Rollen- Berechtigungskonzept • Begrenzung der befugten Benutzer • Kennwortregeln für die Komplexität der Kennwörter (gemäß BSI, zeitliche Limitierung 90 Tage, Groß-/Kleinbuchstaben, Sonderzeichen, Ziffern, Mindestlänge) • BIOS-Passwörter • Identifizierung und Authentifizierung • Protokollierung der Zugriffe • Automatisierte Sperrung der Clients nach definierter Zeit der Inaktivität • Firewall • Anti-Viren Software (unterschiedliche Scanengines)

			• Externer Zugriff über gesicherte VPN Netzwerke • Abgrenzung interner Netze über VLANs • Beschränkung und Überwachung des Netzwerkzugriffs (Radius-Authentifizierung) • Patchmanagement **3. Zugriffskontrolle** Der Unterauftragnehmer stellt sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Berechtigungskonzept • Profile / Rollen • Verfahren zur Vergabe von Berechtigungen • Trennung von Antrag, Bewilligung und Vergabe von Zugriffsrechten • Protokollierung bei Anmeldung • Auswertung der Protokolle • Unterbindung von unbefugtem Überspielen von Daten auf externe Datenträger (Sperrung USB Ports, SD Slots, CD/DVD Brenner etc.) • Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger • Aufbewahrung von Datenträgern in Datentresoren **4. Weitergabekontrolle**

			Der Unterauftragnehmer stellt sicher, dass personenbezogene Daten bei der Weitergabe / Übertragung nicht unbefugt gelesen, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten vorgesehen ist. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Verschlüsselung von Emails bzw. E-Mail Anhängen • Gesicherte Übertragung (z.B. durch Einsatz von SSL, FTPS, TLS) • Protokollierung der Datenübertragung • Einsatz von VPNs • Physikalische Transportsicherung • Regeln für Verpackung und Versand • Regeln für den Umgang mit physischen Datenträgern • Unterbindung von unbefugter Weitergabe von Daten durch Sperrung von USB Ports, SD Slots, CD/DVD Brenner etc. • Mobile Device Management (MDM) **5. Eingabekontrolle** Der Unterauftragnehmer stellt sicher, dass geprüft werden kann, wer personenbezogene Daten eingegeben, verändert oder entfernt hat. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen:

			• Protokollierung sämtlicher Aktivitäten in den Systemen und / oder schriftlich; datenschutzgerechte Aufbewahrung der Protokolle durch den Auftragnehmer für definierten Zeitraum • Löschregeln für Protokolldaten • Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten (Berechtigungskonzept) **6. Auftragskontrolle** Der Unterauftragnehmer stellt sicher, dass personenbezogenen Daten ausschließlich entsprechend den Weisungen des Auftragsgebers verarbeitet werden können. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Schriftlicher Vertrag zur Auftragsdatenverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers • Festlegung von Ansprechpartnern und Verantwortlichen • Kontrolle / Überprüfung der weisungsgebundenen Auftragsdurchführung • Schulung und Einweisung der beteiligten Mitarbeiter • Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß § 53 BDSG **7. Verfügbarkeitskontrolle**

			Der Unterauftragnehmer stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Backup-Verfahren (mit Festlegung von Rhythmus, Medium, Aufbewahrungszeit und -ort) • Redundante Rechenzentren • Spiegelung von Festplatten • Unterbrechungsfreie Stromversorgung (USV) • Stromversorgung über NEA (Netzersatzanlage = Generator) bei Netzausfall • Notfallhandbuch und Notfallkonzept • Alarmanmeldungen bei unberechtigtem Zutritt zu den IT Räumen • Brandschutz und Brandmeldung • Feuerlöschsysteme • Klimatisierung der Serverräume • Patchmanagement • Virenschutz nach dem Stand der Technik • Firewall • Automatisiertes Monitoring der Infrastruktur inkl. Serverräume **8. Trennungskontrolle** Der Unterauftragnehmer stellt sicher, dass zu unterschiedlichen Zwecken erhobene, personenbezogene Daten getrennt verarbeitet

			werden. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Trennung der Systeme • Mandantentrennung • Ordnerstrukturen • Differenzierte Zugriffsregelungen • Trennung von Entwicklungs- und Produktionsumgebung
Westermann GmbH & Co. KG	Technische Betreuung der Anwendung	Georg-Westermann-Allee 66, 38104 Braunschweig	**1. Zutrittskontrolle** Der Unterauftragnehmer stellt sicher, dass Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen haben. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Sicherheitsschlösser mit Schlüsselregelung • verschlossene Türen bei Abwesenheit • Fenstersicherung (insbesondere im Erdgeschoss) • Festlegung von Sicherheitsbereichen • Zutrittskontrollsystem mit Chipkarte sowie ergänzend kontrollierte Schlüsselvergabe • Schließsystem inkl. zeitabhängiger Berechtigungen • Protokollierung der Zu- und Abgänge • Zutrittsregelungen für betriebsfremde Personen inkl. Besucherausweis • Empfang mit Werkschutz und Pförtner

			• Überwachungseinrichtungen der IT Räume mit Alarmanlage • Videoüberwachung **2. Zugangskontrolle** Der Unterauftragnehmer stellt sicher, dass Unbefugt keinen Zugang zu den Datenverarbeitungssystemen haben. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Persönlicher User-Account für die Anmeldung an das Unternehmensnetz und die Systeme • Autorisierungsprozess für die Vergabe von Zugriffsberechtigungen • Regelbasiertes Löschen ausgeschiedener Mitarbeiter • Rollen- Berechtigungskonzept • Begrenzung der befugten Benutzer • Kennwortregeln für die Komplexität der Kennwörter (gemäß BSI, zeitliche Limitierung 90 Tage, Groß-/Kleinbuchstaben, Sonderzeichen, Ziffern, Mindestlänge) • BIOS-Passwörter • Identifizierung und Authentifizierung • Protokollierung der Zugriffe • Automatisierte Sperrung der Clients nach definierter Zeit der Inaktivität • Firewall

			• Anti-Viren Software (unterschiedliche Scanengines) • Externer Zugriff über gesicherte VPN Netzwerke • Abgrenzung interner Netze über VLANs • Beschränkung und Überwachung des Netzwerkzugriffs (Radius-Authentifizierung) • Patchmanagement **3. Zugriffskontrolle** Der Unterauftragnehmer stellt sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Berechtigungskonzept • Profile / Rollen • Verfahren zur Vergabe von Berechtigungen • Trennung von Antrag, Bewilligung und Vergabe von Zugriffsrechten • Protokollierung bei Anmeldung • Auswertung der Protokolle • Unterbindung von unbefugtem Überspielen von Daten auf externe Datenträger (Sperrung USB Ports, SD Slots, CD/DVD Brenner etc.) • Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger • Aufbewahrung von Datenträgern in Datentresoren

			4. Weitergabekontrolle Der Unterauftragnehmer stellt sicher, dass personenbezogene Daten bei der Weitergabe / Übertragung nicht unbefugt gelesen, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten vorgesehen ist. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Verschlüsselung von Emails bzw. E-Mail Anhängen • Gesicherte Übertragung (z.B. durch Einsatz von SSL, FTPS, TLS) • Protokollierung der Datenübertragung • Einsatz von VPNs • Physikalische Transportsicherung • Regeln für Verpackung und Versand • Regeln für den Umgang mit physischen Datenträgern • Unterbindung von unbefugter Weitergabe von Daten durch Sperrung von USB Ports, SD Slots, CD/DVD Brenner etc. • Mobile Device Management (MDM) **5. Eingabekontrolle** Der Unterauftragnehmer stellt sicher, dass geprüft werden kann, wer personenbezogene Daten eingegeben, verändert oder entfernt hat. Der

			Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Protokollierung sämtlicher Aktivitäten in den Systemen und / oder schriftlich; datenschutzgerechte Aufbewahrung der Protokolle durch den Auftragnehmer für definierten Zeitraum • Löschregeln für Protokolldaten • Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten (Berechtigungskonzept) **6. Auftragskontrolle** Der Unterauftragnehmer stellt sicher, dass personenbezogenen Daten ausschließlich entsprechend den Weisungen des Auftragsgebers verarbeitet werden können. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Schriftlicher Vertrag zur Auftragsdatenverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers • Festlegung von Ansprechpartnern und Verantwortlichen • Kontrolle / Überprüfung der weisungsgebundenen Auftragsdurchführung • Schulung und Einweisung der beteiligten Mitarbeiter • Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß § 53 BDSG

			7. Verfügbarkeitskontrolle Der Unterauftragnehmer stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Backup-Verfahren (mit Festlegung von Rhythmus, Medium, Aufbewahrungszeit und -ort) • Redundante Rechenzentren • Spiegelung von Festplatten • Unterbrechungsfreie Stromversorgung (USV) • Stromversorgung über NEA (Netzersatzanlage = Generator) bei Netzausfall • Notfallhandbuch und Notfallkonzept • Alarmanmeldungen bei unberechtigtem Zutritt zu den IT Räumen • Brandschutz und Brandmeldung • Feuerlöschsysteme • Klimatisierung der Serverräume • Patchmanagement • Virenschutz nach dem Stand der Technik • Firewall • Automatisiertes Monitoring der Infrastruktur inkl. Serverräume **8. Trennungskontrolle** Der Unterauftragnehmer stellt sicher, dass zu unterschiedlichen Zwecken erhobene, personenbezogene Daten getrennt verarbeitet

			werden. Der Unterauftragnehmer hat folgende Maßnahmen ergriffen: • Trennung der Systeme • Mandantentrennung • Ordnerstrukturen • Differenzierte Zugriffsregelungen • Trennung von Entwicklungs- und Produktionsumgebung
Gärtner Datensysteme GmbH und Co. KG	Rechenzentrumsbetrieb und technische Entwicklung der Anwendung	Hamburger Straße 273 a, 38144 Braunschweig	**1. Zutrittskontrolle** Ein unbefugter Zutritt zu den Datenverarbeitungsanlagen ist zu verhindern. Folgende Maßnahmen zur Zutrittskontrolle wurden ergriffen: • Sicherheitsschlösser mit Schlüsselregelungen • Verschlossene Türen bei Abwesenheit • Festlegung von Sicherheitsbereichen • Zutrittskontrollsystem mit Chipkarten • Kontrollierte Schlüsselvergabe • Protokollierung der Zu- und Abgänge • Zutrittsregelung für betriebsfremde Personen • Überwachungseinrichtungen der IT-Räume mit Alarmanlage **2. Zugangskontrolle**

			Eine unbefugte Systemnutzung ist zu verhindern. Es wurden folgende Maßnahmen ergriffen: • Persönlicher User-Account für Anmeldungen an das Unternehmensnetz und die Systeme • Regelbasiertes Löschen ausgeschiedener Mitarbeiter • Rollen-Berechtigungskonzept • Begrenzung befugter Nutzer • Firewall • Externer Zugriff über gesicherte VPN-Netzwerke • Abgrenzung interner Netze über VLANs • Patchmanagement **3. Zugriffskontrolle** Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein. Es wurden diesbezüglich folgende Maßnahmen ergriffen: • Berechtigungskonzept • Profile / Rollen • Protokollierung der Anmeldung • Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträgern • Aufbewahrung von Datenträgern in Datentresoren

			4. Trennungskontrolle Zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden getrennt verarbeitet. Diesbezüglich wurden folgende Maßnahmen ergriffen: • Trennung der Systemen • Mandantentrennung • Ordnerstrukturen **5. Weitergabekontrolle** Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein. Außerdem muss prüf- und feststellbar sein, an welchen Stellen eine Übermittlung personenbezogener Daten vorgesehen ist. Hierzu wurden folgende Maßnahmen ergriffen: • Verschlüsselung von E-Mails • Gesicherte Übertragung **7. Eingabekontrolle** Fesstellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

			•Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten **8. Verfügbarkeit und Belastbarkeit** Schutz gegen zufällig oder mutwillig Zerstörung bzw. Verlust wird durch folgende Maßnahmen gewährleistet: • Backup-Verfahren • Redundante Rechenzentren • Spiegelung von Festplatten • Unterbrechungsfreie Stromversorgung • Stromversorgung über NEA bei Netzausfall • Alarmmeldungen bei unberechtigtem Zutritt zu den IT-Räumen • Brandschutz und Brandmeldung • Feuerlöschsysteme • Klimatisierung der Serverräume • Patchmanagement • Firewall • Automatisiertes Monitoring der Infrastruktur inkl. Serverräume **9. Auftragskontrolle**

			Personenbezogene Daten werden ausschließlich entsprechend den Weisungen des Auftraggebers verarbeitet: • Schriftlicher Vertrag zur Auftragsdatenverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers • Festlegung Von Ansprechpartnern und Verantwortlichen • Schulung und Einweisung der beteiligten Mitarbeiter • Verpflichtung der Mitarbeiter auf Vertraulichkeit und Wahrung des Fernmeldegeheimnisses