Vereinbarung

Zwischen dem Verantwortlichen/Auftraggeber:

Beispiel GmbH

-nachstehend Auftraggeber (AG) genannt - und dem Auftragsverarbeiter:

Mitarbeiterschule GmbH, Siemensstraße 12, 48341 Altenberge

-nachstehend Auftragnehmer (AN) genannt- wird die folgende Vereinbarung zur Datenverarbeitung getroffen.

Präambel

Diese Vereinbarung wird unter Beachtung des Bundesdatenschutzgesetzes (BDSG) und der ab 25.05.2018 geltenden EU Datenschutzgrundverordnung (DS-GVO) sowie aller sonstigen einschlägigen datenschutzrechtlichen Vorschriften geschlossen. Für diese Vereinbarung gelten die jeweils in Kraft stehenden Gesetzesvorschriften in ihrer jeweils aktuellen Fassung.

Diese Vereinbarung betrifft die Erhebung, Verarbeitung und Nutzung personenbezogener Daten i.S.d. BDSG und DS-GVO durch den Auftragnehmer im Auftrag des Auftraggebers („Auftragsverarbeitung"). Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person („Betroffener"). Die Vereinbarung hat die Auftragsverarbeitung von personenbezogenen Daten zum Gegenstand („Auftragsdaten").

Vor diesem Hintergrund vereinbaren die Parteien Folgendes:

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der wesentliche Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Übertragung der Mitarbeiterdaten des Auftraggebers zur Abwicklung der webbasierten E-Learning-Lösung.

Der detaillierte Gegenstand des Auftrages ergibt sich aus dem zugehörigen Dienstleistungsvertrag auch Hauptauftrag oder Leistungsvereinbarung genannt.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/- Kategorien (Aufzählung/ Beschreibung der Datenkategorien)

- ✓ Personenstammdaten (Ansprechpartnerliste des AGs, i.d.R. keine Betroffenendaten)
- ✓ Kommunikationsdaten (z.B. Telefon, E-Mail, IP, SM-Accountdaten)
- ✓ Personalstammdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ✓ Beschäftigte des Auftraggebers

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

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

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten.

(4) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer:

   Sebastian Feldmann, Keyed GmbH, s.feldmann@keyed.de

   bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

i) Der Auftragnehmer wird nach den Weisungen des Auftraggebers angemessene Maßnahmen ergreifen, um weitere unrechtmäßige Kenntnisnahmen durch Dritte auszuschließen und/oder weitere Beeinträchtigungen von den Betroffenen abzuwenden. Bis zu etwaigen Weisungen des Auftraggebers wird der Auftragnehmer alle zur Datensicherung und Schadensminimierung erforderlichen Maßnahmen ergreifen.

j) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner gesetzlichen Pflichten, insbesondere Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Informationspflichten gegenüber Betroffenen und Aufsichtsbehörden, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Dasselbe gilt auch dann, wenn der Auftraggeber 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 ausgesetzt ist. Der Auftragnehmer wird dem Auftraggeber auf Anfrage das von ihm nach Maßgabe der einschlägigen Gesetzesvorschriften zu erstellende Verzeichnis aller Verarbeitungstätigkeiten in kopierter Form zur Verfügung stellen.

k) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

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

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**
ALL-INKL.COM, Neue Medien Münnich	Hauptstraße 68, 02742 Friedersdorf, Deutschland	Webhosting der Mitarbeiterschule.de
Heskamp Medien	Borkener Str. 134a, 48653 Coesfeld, Deutschland	IT-Support

c) ☒ Die Auslagerung auf Unterauftragnehmer oder / der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

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

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

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch beispielsweise

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 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).

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

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Die Meldung an den Verantwortlichen bei Schutzverletzungen kann über die üblichen (elektronischen, telefonischen) Kommunikationskanäle getätigt werden vor dem Hintergrund der Meldepflichten wird der schnellstmögliche Informationsaustausch gewährleistet.

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

(4) 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. Zur Haftung gelten die Regelungen des Art. 82 DSGVO.

(5) Der Auftragnehmer seine gesetzlichen Vertreter oder Erfüllungsgehilfen haften nicht bei leichter Fahrlässigkeit. Dieser Ausschluss für die Haftung bei leichter Fahrlässigkeit gilt jedoch dann nicht, wenn es sich um die Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht) handelt. Kardinalpflichten bzw. wesentliche Vertragspflichten sind solche Pflichten des Auftragnehmers, deren Erfüllung die ordnungsgemäße Durchführung dieses konkreten Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf; mithin also Pflichten, deren Verletzung die Erreichung des Vertragszwecks gefährden würde.

9. Weisungsbefugnis des Auftraggebers

Die Entscheidungs- bzw. Weisungsbefugnis für die Auftragsverarbeitung hat allein der Auftraggeber. Der Auftragnehmer wird allein im Auftrag und im Interesse des Auftraggebers tätig. Die Verantwortung für die Einhaltung des Datenschutzrechts und die Rechtmäßigkeit der Auftragsverarbeitung sowie für die Wahrung der Rechte der Betroffenen liegt beim Auftrag-geber.

Der Auftragnehmer führt die Auftragsverarbeitung ausschließlich im Rahmen der Vereinbarung und nach schriftlichen Weisungen des Auftraggebers durch, wobei die Weisungen vorrangig gelten, oder wenn eine gesetzliche Verpflichtung zur Verarbeitung besteht. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen. Der Auftragnehmer ist nicht berechtigt, ohne vorherige schriftliche Zustimmung durch den Auftraggeber Erklärungen gegenüber den Betroffenen abzugeben. Im Falle einer gesetzlichen Verpflichtung teilt der Auftragnehmer dem Auftraggeber diese Verpflichtung vor der Verarbeitung mit.

Der Auftragnehmer darf die Auftragsdaten nicht eigenmächtig, sondern nur nach schriftlicher Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Der Auftragnehmer wird den Auftraggeber über sämtliche Anfragen und Beanstandungen der Betroffenen unverzüglich schriftlich unterrichten sowie den Auftraggeber bei Wahrung der Rechte der Betroffenen unterstützen, wie z.B. durch Benachrichtigung, Auskunftserteilung oder Berichtigung, Sperrung und Löschung von Auftragsdaten.

Die Parteien beachten im Rahmen der Auftragsverarbeitung die einschlägigen datenschutz-rechtlichen Vorschriften. Ist der Auftragnehmer der Ansicht, dass eine Vereinbarung oder Weisung gegen datenschutzrechtliche Vorschriften verstößt, wird er den Auftraggeber hier-über unverzüglich schriftlich informieren. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

(4) Der Auftraggeber und der Auftragnehmer vereinbaren einen Ausschluss des zivilrechtlichen Zurückbehaltungsrechts nach § 273 BGB zum Ausschluss der Zurückhaltung von verarbeiteten personenbezogenen Daten und Datenträgern im Falle von Vertrags-/Leistungsstörungen.

11. Geheimhaltung

Der Auftragnehmer wird die im Rahmen der Auftragsverarbeitung empfangenen Informationen und Unterlagen, insbesondere die Auftragsdaten, streng geheim halten („Geschäfts- und Betriebsgeheimnisse“). Die Geheimhaltungs-/Verschwiegenheitspflichten gelten auch nach Beendigung dieser Vereinbarung unbefristet fort.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

Die Geheimhaltungspflicht gilt nicht oder entfällt, wenn die Informationen und Unterlagen bereits bei Abschluss dieser Vereinbarung der Öffentlichkeit oder dem Auftragnehmer bekannt waren oder nach Abschluss dieser Vereinbarung der Öffentlichkeit bekannt werden, ohne dass den Auftragnehmer hieran ein Verschulden trifft, oder dem Auftragnehmer durch einen Dritten bekannt werden, vorausgesetzt der Dritte verletzt bei Übergabe der Informationen keine eigene Geheimhaltungsverpflichtung. Nachweispflichtig für diese Tatbestände ist der Auftragnehmer.

12. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, 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.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

13. Sonstiges, Allgemeines

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.

Gerichtsstand ist Münster.

(Ort, Datum) (Unterschrift Auftraggeber)

(Ort, Datum) (Unterschrift Auftragnehmer)

Anlage 1 – Technisch-organisatorische Maßnahmen

Zur Information! Diese Angaben entsprechen unter Umständen nicht den tatsächlichen Maßnahmen.

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

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 2 – technische und organisatorische Maßnahmen

„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,...“		
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)		
Zutrittskontrolle	*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*	✓ Absicherung von Gebäudeschächten ✓ Automatisches Zugangskontrollsystem ✓ Manuelles Schließsystem ✓ Lichtschranken / Bewegungsmelder ✓ Sicherheitsschlösser ✓ Schlüsselregelung (Schlüsselausgabe etc.) ✓ Personenkontrolle beim Empfang ✓ Sorgfältige Auswahl von Reinigungspersonal ✓ Sorgfältige Auswahl von Wachpersonal
Zugangskontrolle	*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*	✓ Zuordnung von Benutzerrechten ✓ Erstellen von Benutzerprofilen ✓ Passwortvergabe ✓ automatische Sperrmechanismen ✓ Authentifikation mit Benutzername / Passwort ✓ Zuordnung von Benutzerprofilen zu IT-Systemen ✓ Gehäuseverriegelungen ✓ Einsatz von VPN-Technologie ✓ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

		✓ Einsatz von Anti-Viren-Software ✓ Einsatz einer Hardware-Firewall ✓ Einsatz einer Software-Firewall
Zugriffskontrolle	*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*	✓ Identifizierungs- und Authentifizierungssystem ✓ Erstellen eines Berechtigungskonzepts ✓ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten ✓ Verschlüsselungsverfahren/-systeme ✓ Vier-Augen-Prinzip bei Spezialanwendungen ✓ Sichere Aufbewahrung von Datenträgern (Datentresor) ✓ Verschlüsselung von Datenträgern ✓ physische Löschung von Datenträgern vor Wiederverwendung ✓ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399) ✓ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) ✓ Protokollierung (der Vernichtung) zum Nachvollzug
Trennungskontrolle	*Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist zu garantieren!*	✓ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern ✓ Logische Mandantentrennung (softwareseitig) ✓ Rechteverwaltung bzw. Erstellung eines Berechtigungskonzepts ✓ Festlegung von Datenbankrechten ✓ Verschlüsselung von Datensätzen, die zu

		demselben Zweck verarbeitet werden ✓ Versehen der Datensätze mit Zweckattributen/Datenfeldern ✓ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System ✓ Trennung von Produktiv- und Testsystem ✓ Sandboxing ✓ Protokollierung und Beweissicherung
Pseudonymisierung	*Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.*	

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)		
Weitergabekontrolle	*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*	✓ Einrichtungen von Standleitungen bzw. VPN-Tunneln ✓ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form ✓ Regelung / Dokumentation Ausgabe- und Empfängerkreis ✓ Fernwartungskonzept ✓ Beim physischen Transport: sichere Transportbehälter/-verpackungen ✓ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -Fahrzeugen

Eingabekontrolle	*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*	✓ Identifizierung und Authentifizierung ✓ Dokumentenmanagement ✓ Protokollierung der Eingabe, Änderung und Löschung von Daten ✓ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. ✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) ✓ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)		
Verfügbarkeitskontrolle	*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind*	✓ Virenschutz ✓ Firewall / IDS ✓ Unterbrechungsfreie Stromversorgung (USV) ✓ Klimaanlage in Serverräumen ✓ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen ✓ Schutzsteckdosenleisten in Serverräumen ✓ Feuer- und Rauchmeldeanlagen ✓ Feuerlöschgeräte in Serverräumen

		✓ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen ✓ Backup-Strategie (online/offline; on-site/off-site) ✓ Verfügbarkeit eines Notfall-RZ ✓ Erstellen eines Backup- und Recovery-Konzepts ✓ Testen von Datenwiederherstellung ✓ Erstellen eines Notfallkonzeptes / Notfallplans ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort ✓ Serverräume nicht unter sanitären Anlagen
Wiederherstellbarkeit	*Maßnahmen, die die rasche Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust oder Beschädigung gewährleisten.* Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)	✓ Backup-Strategie (online/offline; on-site/off-site) ✓ Verfügbarkeit eines Notfall-RZ ✓ Erstellen eines Backup- und Recovery-Konzepts ✓ Testen von Datenwiederherstellung ✓ Erstellen eines Notfallkonzeptes / Notfallplans ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)		
Datenschutz-Management		
Incident-Response-Management		
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)	*Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher*	✓ Pseudonymisierung ✓ Beschränkung bzgl. der Menge der erhobenen Auftragsdaten

	Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. *Data Privacy by Design and by Default*	✓ Beschränkung des Umfangs der Verarbeitung der erhobenen Daten ✓ Beschränkung der Speicherfrist ✓ Beschränkung der Zugänglichkeit
Auftragskontrolle	*Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeitet werden (können)!*	✓ Eindeutige Vertragsgestaltung / vertragliche Regelungen ✓ Formalisiertes Auftragsmanagement ✓ Strenge Auswahl des Dienstleisters (insbesondere hinsichtlich Datensicherheit) ✓ Vorabüberzeugungspflicht ✓ Vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen ✓ Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d.Art. 28 DS-GVO ✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 53 BDSG) ✓ Auftragnehmer hat Datenschutzbeauftragten bestellt ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags ✓ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart ✓ Vertragsstrafen bei Verstößen

Geprüft durch Keyed GmbH in Münster und Düsseldorf am 19.02.2019.

Auditor: Sebastian Feldmann