Vertrag zur Auftragsverarbeitung

zwischen

_____
_____
_____

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und der

foreknown GmbH
Brückenstr. 7
48231 Warendorf

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen, welche die Verarbeitung von personenbezogenen Daten umfassen. Dabei stellt insbesondere Art. 28 Datenschutzgrundverordnung (DSGVO) bestimmte Anforderungen an eine Auftragsverarbeitung, wie sie Gegenstand der in § 3 genannten Leistungen sein soll. Um diesen Anforderungen Genüge zu tun, schließen die Parteien die nachfolgende Vereinbarung ab, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Die Vereinbarung dient der Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten.

§ 1 Begriffsbestimmungen

(1) Verantwortliche im Sinne der DSGVO ist diejenige Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art.4 Abs.7 DSGVO).

(2) Auftragsverarbeiter im Sinne der DSGVO ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art.4 Abs.8 DSGVO).

(3) Personenbezogene Daten im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art.4 Abs.1 DS-GVO).

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen (Art.9 DSGVO), personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln (Art.10 DSGVO) sowie genetische Daten (Art.4 Abs.13 DSGVO), biometrische Daten (Art.4 Abs.14 DSGVO), Gesundheitsdaten (Art.4 Abs.15 DSGVO) sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art.4 Abs.2 DSGVO).

(6) Aufsichtsbehörde ist eine von einem Mitgliedstaat gem. Art.51 DSGVO eingerichtete unabhängige staatliche Stelle (Art.4 Abs.21 DSGVO).

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Beratung und Entwicklung von Software und ist auf Grundlage der

Nutzungsbedingungen Foreknown („Hauptvertrag“)

vom _____ (Datum: Abschluss des Hauptvertrages)

Dienstleister im Bereich des Cloud-Computing. In diesem Rahmen bietet er das sog. Software as a Service“-Modell (SaaS-Modell) an, betreibt also als externer IT-Dienstleister die Software und IT-Infrastruktur des Auftraggebers. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag.

(2) Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages 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 vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; 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 dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können danach von den weisungsberechtigten Personen des Auftraggebers, wie sie sich aus Anlage 5 ergeben, in schriftlicher Form oder in Textform gegenüber dem Auftragnehmer durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Die Weisungen sind schriftlich oder in Textform zu bestätigen. Sie haben eine angemessene Frist zur Umsetzung beim Auftragnehmer zu berücksichtigen.

(3) Vom Weisungsrecht umfasst sind Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Bei einem Wechsel oder einer längerfristigen Verhinderung der in Anlage 5 benannten weisungsberechtigten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Das Versäumnis unverzüglicher Mitteilung eines Wechsels und seiner Konsequenzen fällt nicht in den Risikobereich des Auftragnehmers, sondern liegen in der Risikosphäre des Auftraggebers.

(4) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt, der eine Annahme durch den Auftragnehmer voraussetzt.

(5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(6) Liegt in der Sphäre des Auftragnehmers eine Rechtswidrigkeit vor und würde er vorsätzlich in ordnungswidriges oder strafbares Handeln involviert, darf er mit Blick auf das Straf- und Haftungsrisiko die Weisung ablehnen.

(7) Die Durchführung einer offensichtlich rechtswidrigen Weisung darf der Auftragnehmer immer ablehnen. Offensichtlich rechtswidrig ist eine Weisung insbesondere dann, wenn eine Rechtsgrundlage für die Verarbeitungstätigkeit unter Berücksichtig der einschlägigen datenschutzrechtlichen Bestimmungen nicht in Betracht kommt.

§ 4 Verpflichtung zur Zusammenarbeit mit der zuständigen Datenschutz-Aufsichtsbehörde

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

(2) Zuständige Aufsichtsbehörde für den Auftraggeber ist der Landesbeauftragte für den Datenschutz _____.

(3) Zuständige Aufsichtsbehörde für den Auftragnehmer ist der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen die in Anlage 1 aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten

Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Zweckbindungskontrolle, Weitergabekontrolle, Eingabekontrolle und Verfügbarkeitskontrolle. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Ansprechpartner für den Datenschutz sind die Geschäftsführer des Auftragnehmers, Herr Andreas grosse Austing und Herr Bernfried Howe.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden „Mitarbeiter“ genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art.28 Abs.3 lit.b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) 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 den Auftraggeber unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) 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, 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 beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs.2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art.30 Abs.2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer mitzuwirken, indem er dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitteilt.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig einmal im Jahr von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er 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 nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer innerhalb von drei Wochen mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber

feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.Der Auftragnehmer stellt dem Auftraggeber auf dessen schriftlich geäußerten Wunsch daraufhin ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung. Das gilt auch für den Fall, dass dies im Rahmen eines behördlichen Aufsichtsverfahrens für den Auftraggeber erforderlich wird, da Gegenstand des Aufsichtsverfahrens die Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer ist.

(4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs.4 auf schriftliches Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich zugestimmt hat. 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 und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) 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 den Auftraggeber 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 den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art.12–22, 32 und 36 DSGVO. Die Maßnahmen sind einzelfallabhängig zwischen den Vertragsparteien zu besprechen. Sie müssen sich nach dem Umfang der Leistungspflichten aus dem Hauptvertrag richten und finden unter Berücksichtigung der Tatsache statt, dass dem Auftraggeber die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab. Erfolgt eine solche Weisung nach Anzeige nicht innerhalb eines angemessenen Zeitraumes mit Blick auf das geltend gemachte Betroffenenrecht, fallen die daraus resultierenden rechtlichen Konsequenzen nicht in den Risikobereich des Auftragnehmers, sondern liegen in der Risikosphäre des Auftraggebers.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 Außerordentliches Kündigungsrecht

(1) Die Vertragsparteien können diesen Vertrag jederzeit außerordentlich aus wichtigem Grund kündigen.

(2) Ein wichtiger Grund liegt für den Auftraggeber insbesondere dann vor, wenn

- der Auftragnehmer Bestimmungen nach der DSGVO vorsätzlich oder grob fahrlässig verletzt,
- der Auftragnehmer Weisungen des Auftraggebers, wie in § 4 dieses Vertrages beschrieben, entgegen

seiner vertraglichen Pflichten nicht nachkommen will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen gegen die Bestimmungen der DSGVO oder Pflichten aus diesem Vertrag setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

(3) Ein wichtiger Grund liegt für den Auftragnehmer insbesondere dann vor, wenn die Weisungen des Auftraggebers nach § 4 dieses Vertrages offensichtlich rechtswidrig sind und der Auftraggeber auf der Durchführung seiner Weisung nach Hinweis auf deren Rechtswidrigkeit beharrt. Bei einfachen – also nicht offensichtlich rechtswidrigen – Verstößen setzt der Auftragnehmer dem Auftraggeber eine angemessene Frist, innerhalb welcher der Auftraggeber die Weisung schriftlich oder in Textform abstellen kann.

(4) Eine vom Hauptvertrag isolierte Kündigung dieses Vertrages ist ausgeschlossen.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, 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 Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen 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 vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf diese Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(2) 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.

(3) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Münster.

Anlagen:

Anlage 1 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien
Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen
Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers
Anlage 4 – Genehmigte Subunternehmer
Anlage 5 – Weisungsberechtigte Personen

_____	_____
Datum, Unterschrift Auftraggeber	Datum, Unterschrift Auftragnehmer

Anlage 1 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

- Benutzerdaten (E-Mail und Passwort (gehasht))
- Personenstammdaten (Vorname, Nachname, Adresse)
- Mitarbeiterdaten (Name, E-Mail, Standort)
- Kundendaten (Name, E-Mail, Anschrift, Ansprechpartner)

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Beschreibung der technischen und organisatorischen Maßnahmen des Auftragnehmers für:

Pseudonymisierung

Die Daten, die durch den Auftraggeber in die Software eingegeben werden, können durch den Auftraggeber nicht pseudonymisiert werden.

Werden jedoch Daten von der Entwicklungsabteilung des Auftragnehmers benötigt, um einen spezifischen Fehler des Auftraggebers in der Software zu reproduzieren, werden diese pseudonymisiert, um keine Rückschlüsse auf Informationen zu realen Personen (Mitarbeiter- und Kundenkontakte) sowie Kundennamen- und Projektnamen schließen zu können. Dies betrifft folgende Daten:

- Benutzerdaten (E-Mail und Passwort)
- Personenstammdaten (Vorname, Nachname, Adresse)
- Mitarbeiterdaten (Name, E-Mail)
- Kundendaten (Name, E-Mail, Anschrift, Ansprechpartner)

Verschlüsselung

- Der Zugriff auf die Software erfolgt über den Webbrowser. Die Daten werden verschlüsselt übertragen (SSL).
- Passwörter werden gehasht in der Datenbank abgelegt.
- Dateien, die über die Weboberfläche hochgeladen werden, werden verschlüsselt im Dateisystem des Servers gespeichert.
- Backups der Datenbank und der Daten werden verschlüsselt gespeichert.

Vertraulichkeit

Zutrittskontrolle

Die zum Betrieb der Software notwendigen Server werden bei der die Hetzner Online GmbH betrieben. Die Zugriffskontrolle wird durch die Hetzner Online GmbH wie folgt gewährleistet (Vgl. https://accounts.hetzner.com/downloads/dpa2-de.pdf):

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters

Zugangskontrolle

- Der Zugriff auf die Weboberfläche der Software ist passwortgeschützt. Das Passwort wird durch die zugriffsberechtigten Personen des Auftraggebers selbst vergeben. Der Auftragnehmer hat keinen Zugriff auf die Klartext-Passwörter. Lediglich zur ersten Anmeldung am System wird ein Passwort generiert und dem Auftraggeber zugesandt. Der Auftraggeber ist verpflichtet, dieses Passwort nach der ersten Anmeldung zu ändern.
- Der Zugriff auf die Server ist durch den Auftragnehmer nur mittels eines gesicherten Verfahrens (SSH) möglich. Die hierzu benötigten Passwörter/Zugriffsschlüssel sind in einer speziellen Sicherheitsanwendung verschlüsselt hinterlegt. Nur durch den Auftragnehmer autorisierte Personen dürfen auf diese Anwendung und damit auf die Server zugreifen.

Zugriffskontrolle

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.

Trennungskontrolle und Zweckbindungskontrolle

- Die Software ist mandantenfähig, d.h. die Daten eines Mandanten sind nicht durch einen anderen Mandanten zugreifbar. Die Trennungskontrolle zwischen den Mandanten ist in der Software implementiert (Logische Trennung).
- In der Testphase der Software wird für den Auftraggeber ein neuer Mandant auf dem “Demo-System” eingerichtet (Logische Trennung).
- Nach der Testphase wird für den Auftraggeber ein eigener Server bereitgestellt. Alle Daten sind physisch getrennt voneinander gespeichert (Physische Trennung).

Verfügbarkeit, Belastbarkeit

Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme).
- Einsatz von Festplattenspiegelung bei allen relevanten Servern (durch Hetzner).
- Monitoring aller relevanten Server.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage (durch Hetzner).
- Dauerhaft aktiver DDoS-Schutz (durch Hetzner).

Wiederherstellbarkeit

- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

Integrität

Weitergabekontrolle

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

Eingabekontrolle

- Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.
- Die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird durch die Verantwortlichen für den Datenschutz regelmäßig überprüft, bewertet und evaluiert und an den Stand der Technik angepasst.

Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

- Hetzner Online GmbH
  Industriestr. 25
  91710 Gunzenhausen
  Deutschland

Anlage 5 – Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers sind:

- _____
- _____

Weisungsempfänger beim Auftragnehmer sind:

- Andreas grosse Austing
- Bernfried Howe