Vertrag zur Auftragsverarbeitung

Zwischen

der

Firma, Anschrift, Vertretungsberechtigter

als Verantwortlicher

(hier bezeichnet als „***Auftraggeber***“)

und

der **Ryte GmbH**, Paul-Heyse-Straße 27, 80336 München

als Auftragsverarbeiter

(hier bezeichnet als „***Auftragnehmer***“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

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

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO 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.

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

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO 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.

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

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Aufsichtsbehörde für den Auftraggeber ist die Name, Kontaktdaten einfügen

(2) Zuständige Aufsichtsbehörde für den Auftragnehmer ist das Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Promenade 18, 91522 Ansbach, Telefon: +49 (0) 981 180093-0, Telefax: +49 (0) 981 180093-800, E-Mail: poststelle@lda.bayern.de

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich “Webservices”. 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. Auf den Hauptvertrag wird vollumfänglich Bezug genommen. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) 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 darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 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 vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigte Person auf Seiten des Auftraggebers ist Name, Kontaktdaten einfügen . Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) 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.

(4) 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. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die im Folgenden näher spezifizierten personenbezogenen Daten. Diese Daten umfassen:

- Vor- und Nachname(n)
- IP-Adressen
- Anschrift
- Telefonnummer
- Emailadresse
- Firma des Arbeitgebers
- Berufliche Tätigkeit

(2) Der Kreis der von der Datenverarbeitung Betroffenen umfasst:

- Mitarbeiter/-innen des Auftraggebers

§ 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 DS-GVO

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als externer Datenschutzbeauftragter für den Datenschutz bestellt: ECOVIS L+C, Dr. Larissa von Paulgerg. Christoph-Rapparini-Bogen 25, 80639 München, dsb-muenchen(at)ecovis.de, +4989217516-700. Der Auftragnehmer hat die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite veröffentlicht.

(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 DS-GVO) 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 in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest 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 von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(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 DS-GVO 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 externen Datenschutzbeauftragten 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 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 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 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

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

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO; und/oder
- die Zertifizierung nach einem Zertifizierungsverfahren gemäß Art. 42 DSGVO; und/oder
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); und/oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Der Aufwand einer Kontrolle beim Auftragnehmer ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Für zusätzliche Kontrollen, denen nicht ein konkreter Anlass oder ein begründeter Verdacht der Verletzung personenbezogener Daten zu Grunde liegt, kann der Auftragnehmer eine angemessene Vergütung verlangen.

§ 9 Einsatz von Subunternehmern

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, vgl. Art. 28 Abs. 2 DSGVO.

(2) Die Genehmigung ist dem Auftragnehmer zu erteilen, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift, sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt und dieser die Voraussetzungen des § 9 Abs.3 und Abs. 4 dieses Vertrages erfüllt.

(3) Der Auftragnehmer verpflichtet sich dazu, den Subunternehmer sorgfältig auszuwählen und insbesondere bereits im Vorfeld dessen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO auf Ihre Wirksamkeit zu prüfen und dies zu dokumentieren.

Das Ergebnis der Dokumentation und die wesentlichen Inhalte sind dem Auftraggeber auf sein Verlangen hin vorzuzeigen.

(4) Die Beauftragung von Subunternehmern, welche Ihren Sitz in Drittstaaten haben, werden nur unter den gesonderten Bestimmungen der Art. 44 ff. DSGVO kontrahiert. Diesbezüglich hat der Auftragnehmer, dem Auftraggeber entsprechende Nachweise auf Verlangen aufzuzeigen. Dies mit Hilfe der EU-Standardvertragsklauseln erfolgen. Rein deklaratorisch ist festzuhalten, dass diese Verträge schriftlich oder gemäß der DSGVO nach Art. 28 Abs. 4 und Abs. 9 im elektronischen Format abzufassen sind.

(5) Der Auftragnehmer verpflichtet sich, im Rahmen seines möglichen, die Einhaltung der datenschutzrechtlichen Pflichten seines Subunternehmers zu überprüfen, dies zu dokumentieren und auf Verlangen des Auftraggebers die wesentlichen Teile der Dokumentation auszuhändigen.

(6) Entsprechend der vorgelagerten Präambel i.V.m. § 3 des Vertrages, sind dem Auftraggeber die Vielzahl der Subunternehmer auf Seiten des Auftragnehmers bewusst. Dem besonderen Geschäftsfeld des Auftragnehmers geschuldet, sind diese zur vollumfänglichen Vertragserfüllung auch erforderlich. Dem einhergehend sind im Zeitpunkt des Abschluss des AVV, die Subunternehmer, seitens des Auftragnehmers bekannt. Diese werden nach folgendem Raster geführt: „Supplier“, „Address“ „DPA-Status“ und „Content“ geführt. Mit Unterzeichnung des vorliegenden Vertrages, genehmigt der Auftraggeber vollumfänglich die in der Liste bezeichneten Subunternehmer.

(7) Ferner verpflichtet sich der Auftragnehmer, dem Auftraggeber jede wesentliche Änderung in Bezug auf eine mögliche Erweiterung, Ersetzung oder Streichung einzelner Subunternehmer anzuzeigen. Dem Auftraggeber wird hierbei das Gestaltungsrecht in Form eines Einspruch (Art 28 Abs.2 S.2 DSGVO) zugebilligt, welches sich explizit auf die Erweiterung, also die Hinzunahme eines gänzlich neuen Subunternehmers für eine bisweilen nicht erbrachte Leistung, und die Ersetzung eines bisherigen Subunternehmers bezieht. Die unternehmerische Entscheidungshoheit des Auftragnehmers wird hierdurch nicht tangiert.

(8) Der Auftraggeber hat nach Anzeige des Auftragnehmers, diesem innerhalb von drei Wochen anzuzeigen, ob er von seinem Einspruchsrecht gebrauchen machen wird. Hierfür ist zumindest Textform und bei Ausübung seines Rechts die Angabe eines wichtigen Grundes für den Einspruch erforderlich. Sollte der Auftraggeber – gleich aus welchem Grunde – sein Recht nicht gegenüber dem Auftragnehmer rechtzeitig ausüben, gilt mit Ablauf des dritten Werktags, der angezeigte Subunternehmer als genehmigt und wird der Liste der Subunternehmer hinzugefügt.

(9) Für eine weitere Auslagerung durch einen Unterauftragnehmer, gilt entsprechend der oben festgelegte Ablauf.

(10) Ein Subunternehmerverhältnis im Sinne dieser Bestimmung liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sein. Dazu gehören bspw. Post-, Transport-, Reinigungs-, Telekommunikations- und Versandleistungen, die nicht im konkreten Austauschverhältnis zur Hauptleistungspflicht stehen.

§ 10 Anfragen und Rechte Betroffener,

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(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.

§ 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, es sei denn der Verstoß gegen geltende Datenschutzbestimmungen und Gesetze und/oder diesen Vertrag liegt im Verantwortungsbereich des Auftragnehmers.

(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

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 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 zu vernichten. Zu entsorgende Datenträger sind nach unwiederbringlich 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) 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.

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

(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.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist München, Deutschland.

Ort , den Datum ……

München, den Datum ……

……...

Für die Auftraggeber

……...

Für die Ryte GmbH

Technische und organisatorische Maßnahme

Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

---

1. Maßnahmen zur Sicherung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- x Schlüsselregelung (Schlüsselausgabe etc.)
- x Protokollierung der Besucher
- x Chipkarten-/Transponder-Schließsystem
- x Manuelles Schließsystem
- x Sicherheitsschlösser
- x Sorgfältige Auswahl von Reinigungspersonal

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- x Zuordnung von Benutzerrechten
- x Passwortvergabe
- x Authentifikation mit Benutzername / Passwort
- x Sperren von externen Schnittstellen (USB etc.)
- x Schlüsselregelung (Schlüsselausgabe etc.)
- x Protokollierung der Besucher
- x Einsatz von Anti-Viren-Software
- x Einsatz einer Hardware-Firewall
- x Erstellen von Benutzerprofilen
- x Zuordnung von Benutzerprofilen zu IT-Systemen
- x Einsatz von VPN-Technologie
- x Sicherheitsschlösser
- x Sorgfältige Auswahl von Reinigungspersonal
- x Verschlüsselung von Datenträgern in Laptops / Notebooks
- x Einsatz einer Software-Firewall

1.3 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.

x	Erstellen eines Berechtigungskonzepts	x	Verwaltung der Rechte durch Systemadministrator
x	Anzahl der Administratoren auf das „Notwendigste“ reduziert	x	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
x	Physische Löschung von Datenträgern vor Wiederverwendung	x	Sichere Aufbewahrung von Datenträgern
x	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)	x	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
x	Verschlüsselung von Datenträgern	x	Protokollierung der Vernichtung

1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

x	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	x	Logische Mandantentrennung (softwareseitig)
x	Erstellung eines Berechtigungskonzepts	x	Trennung von Produktiv- und Testsystem
x	Versehen der Datensätze mit Zweckattributen/Datenfeldern	x	Festlegung von Datenbankrechten

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a; Art. 25 Abs. 1 DSGVO)

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

x	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren

2. Maßnahmen zur Sicherung der Integrität (Art. 32 Abs. 1 lit b DS-GVO)

2.1 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 sowie Maßnahmen mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist. (d.h. Kein unbefugtes Lesen, kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur).

x	E-Mail-Transportverschlüsselung	x	Verwaltung der Rechte durch Systemadministrator
x	Einsatz von VPN	x	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
x	Bereitstellung über verschlüsselte Verbindung	x	Sorgfalt bei der Auswahl von Transportpersonal und -Fahrzeugen

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. (z.B. Protokollierung, Dokumentenmanagement).

Beschreibung des Eingabekontrollvorgangs:

x	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können	x	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
x	Klare Zuständigkeiten für Löschungen		

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

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- x Unterbrechungsfreie Stromversorgung (USV)
- x Schutzsteckdosenleisten in Serverräumen
- x Feuer- und Rauchmeldeanlagen
- x Serverräume nicht unter Sanitärenanlagen
- x Festlegung von Datenbankrechten

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs.1 lit. c DS-GVO)

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

- x Testen von Datenwiederherstellung
- x Vorliegen eines Backup- & Recovery-Konzepts
- x Vorliegen eines Notfallplans

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

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

4.1 Datenschutzmanagement

x	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (z.B. Wiki, Intranet)	x	Interner/externer IT-Sicherheitsbeauftragter
x	Interner/externer Datenschutzbeauftragter	x	Informationspflichten gem. Art. 13 und 14 DS-GVO werden erfüllt
x	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet	x	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

x	Einsatz von Firewall und regelmäßige Aktualisierung	x	Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
x	Dokumentierter von Sicherheitsvorfällen und Datenpannen	x	Einbindung des Sicherheitsbeauftragten in Sicherheitsvorfälle und Datenpannen

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

Privacy by design / Privacy by default.

x	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	x	Einfache Auslegung des Widerrufsrechts des Betroffenen durch technische und organisatorische Maßnahmen

4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartungen und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

x	Überprüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation vor Beauftragung	x	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten insbesondere in Bezug auf Datenschutz und Datensicherheit
x	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln	x	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
x	Schriftliche Weisungen an den Auftragnehmer	x	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht
x	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer	x	Regelungen zum Einsatz weiterer Subunternehmer
x	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	x	Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

München, den 16. Oktober 2019

Ryte GmbH

_____

Andreas Bruckschlögl
Geschäftsführer / Managing Director

Ryte GmbH
Paul-Heyse-Str. 27
80336 Munich, Germany
www.ryte.com

Contact
Phone: +49 89-4161151-0
Fax: +49 89-4161151-19
E-Mail: info@ryte.com

Managing directors
Andreas Bruckschloegl
Marcus Tandler

Bank details
IBAN: DE16 7025 0150 0022 9176 60
BIC: BYLADEM1KMS
Kreissparkasse München Starnberg Ebersberg

Tax & Legal
VAT-ID: DE284700490
District court: Munich
Register number: HRB 200042