Vereinbarung zur Auftragsverarbeitung nach EU-Datenschutz-Grundverordnung (DS-GVO)
(Elektronischer Abschluss)

Zwischen

- Auftraggeber -

und

Buhl Data Service GmbH
Am Siebertsweiher 3/5
57290 Neunkirchen

- Auftragnehmer -

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO). Etwaige zwischen den Parteien zur alten Rechtslage geschlossenen Verträge (Auftragsdatenverarbeitung gemäß § 11 BDSG) werden beendet und durch diesen Vertrag ersetzt.

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag zur Leistungserbringung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag zur Leistungserbringung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten. Bei mehreren Hauptverträgen umfasst die Vereinbarung alle Auftragsverarbeitungen des Auftragnehmers, für die ein jeweiliger Vertrag zur Leistungserbringung mit dem Auftraggeber besteht (nach Login abrufbar im Kundenkonto des Auftraggebers unter www.buhl.de).

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Hauptvertrag zur Leistungserbringung ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

(1) Art der Daten:

Art der personenbezogenen Daten sind alle Arten personenbezogener Daten, die der Auftragnehmer im Auftrag des Kunden verarbeitet. Insbesondere sind dies:

a. Personenstammdaten (z.B. Name und Anschrift, Bild)
b. Kommunikationsdaten (z.B. Telefon, E-Mail)
c. Vertragsstammdaten (z.B. Abrechnungs- und Zahlungsdaten, Bankverbindung)
d. Kundenhistorie
e. Nutzungsdaten
f. Kenndaten (z.B. Steueridentifikationsnummer, Ausweisnummer)

Hiervon umfasst sein können auch besondere Kategorien personenbezogener Daten.

(2) Art und Zweck der Datenverarbeitung

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DS-GVO.

Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung erforderlichen Zwecke. Dies sind insbesondere:

a. Bereitstellung von IT-Infrastruktur, sowie Speicherung und Sicherung der Daten im Rahmen der Cloud-Hosting-Dienste des Auftragnehmers
b. Diagnose und Wartung per Fernzugriff, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Kategorien betroffener Personen

Kategorien betroffener Personen sind insbesondere

c. Kunden, Interessenten des Auftraggebers
d. Beschäftigte des Auftraggebers (z.B. Ansprechpartner)
e. Personen, deren Daten der Auftragnehmer im Auftrag verarbeitet (z.B. Mieter, Vereinsmitglieder, Lieferanten)

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages zur Leistungserbringung, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag zur Leistungserbringung und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Hauptvertrag zur Leistungserbringung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag zur Leistungserbringung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(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 Art. 33 bis 36 DS-GVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) 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) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Hauptvertrages zur Leistungserbringung anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Hauptvertrag zur Leistungserbringung bereits vereinbart.
In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Hauptvertrag zur Leistungserbringung bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich.

Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Hauptvertrages zur Leistungserbringung anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten, kann der Auftragnehmer, dem Auftraggeber insbesondere folgende Informationen zur Verfügung vorlegen:

   a. Durchführung eines Selbstaudits

   b. unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung

   c. Zertifikat zu Datenschutz und/oder Informationssicherheit (z. B. ISO 27001)

   d. genehmigte Verhaltensregeln nach Art. 40 DS-GVO

   e. Zertifikate nach Art. 42 DS-GVO

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein

Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Hauptvertrag zur Leistungserbringung vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Hauptvertrag zur Leistungserbringung vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. für Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software in Anspruch nimmt, sofern ein Zugriff auf personenbezogene Daten ausgeschlossen werden kann.

(3) Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen.

§ 8 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 Vereinbarung 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 Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages zur Leistungserbringung vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

(1) Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.
(2) Soweit keine Haftungsregelung vereinbart wurde, haften Auftraggeber und Auftragnehmer gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Hinweis: Diese Vereinbarung erfolgt mittels elektronischer Zustimmung.

Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Kontrollziele	**Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen**
Pseudonymisierung und Verschlüsselung personenbezogener Daten	• HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport) • obligatorische Verschlüsselung aller administrativen Zugriffe • Obligatorische Verschlüsselung aller ausgehenden E-Mails • Verwendung einer speziellen Hardware-Verschlüsselung für besonders kritische Daten (HSM) • Verschlüsselung aller Datensicherungsbänder
Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	• Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern, • Obligatorische Mehr-Faktor-Authentifizierung für Fernzugriffe • Zentraler selbst-gehosteter individueller Passwort-Safe für alle Beschäftigte • Berechtigte können nur auf für sie berechtigte Daten zugreifen, • personenbezogene gespeicherte Daten können nur im Rahmen der Berechtigungsstufen gelesen, kopiert, verändert oder entfernt werden, • Einsatz eines Firewall- und Web-Application-Firewallsystems • Ausschließliche Verwendung der vom Hersteller der Hardware und Virtualisierungssoftware freigegebenen Software, • Verpflichtung der Mitarbeiter auf das Datengeheimnis • Redundante Klimaanlagen, redundante USVs in Serverräumen • Alert-Meldung bei Ausfällen der Serversysteme • Virtualisierung/Dynamische Zuteilung der Anwendung auf getrennte Serverräumen • Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen des Rechenzentrums, • Besucher der Rechenzentren (z.B. für Wartungszwecke) werden zwingend begleitet • Festlegung der berechtigten Personen für die sensiblen Bereiche der Rechenzentren Einbruchschutzmaßnahmen, Alarmanlage mit Aufschaltung auf Wachdienst • Besonderer Perimeterschutz für RZ-Bereiche • Protokollierung des Zutritts zu den Rechenzentren über entsprechende Transponder • Sichere Löschung von Datenträgern. • Videoüberwachung (Empfang und RZs), • Regelungen zur Kontrolle von externer Wartung und Fernwartung • Brandfrüherkennung und Gas-Löschanlage in besonderen RZ-Bereichen • Brandmeldeanlage mit Aufschaltung auf Feuerwehrleitstelle • Redundante Internetanbindung mit erdkabelfreier Breitband-Fallback-Anbindung • Schutz vor Netz-Überlastungsangriffen (DDoS) auf TIER 1-Ebene

Kontrollziele	**Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen**
Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	• Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung (z. B. Datensicherung und Spiegelung von Hardwarekomponenten); • Datensicherungs- und Recoverykonzept • Auslagerung von Backups zu einem entfernten, eigenen Disaster-Recovery Standort umgehend nach Erstellung • besonders geschützte Rechenzentrumsabschnitte in getrennten Brandabschnitten und Gebäuden • unterbrechungsfreie Stromversorgung, • Überwachungs- und Meldesysteme, • Netzersatzanlage (NEA)
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitung	• Regelmäßige Prüfung, ob/in welchem Umfang Zugangsrechte noch erforderlich sind, • Regelmäßige Prüfung, ob/in welchem Umfang Zugriffsrechte noch erforderlich sind, • Incident-Response-Management • Auftragskontrolle bei Auftragsverarbeitung • Regelmäßige Ausfalltests der Infrastrukturkomponenten