Anlage zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

zwischen

FIO SYSTEMS AG
Ritter-Pflugk-Str. 24
04249 Leipzig

- im Folgenden "FIO SYSTEMS" –

und

Firma
Straße Hausnummer
PLZ Ort

- im Folgenden "Auftraggeber" -

1. Allgemeines zu Datenschutz

(1) FIO SYSTEMS wird im Rahmen der Vertragserfüllung als Auftragsverarbeiter gemäß Art. 28 der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 (nachfolgend EU-Datenschutzgrundverordnung bzw. EU-DSGVO) tätig. FIO SYSTEMS wird die Grundsätze ordnungsgemäßer Datenverarbeitung sowie die Bestimmungen des EU-DSGVO und der ab dem 25. Mai 2018 geltenden Fassung des BDSG (nachfolgend BDSG-neu) beachten und ihre Einhaltung laufend überwachen. FIO SYSTEMS gewährleistet die im Rahmen der ordnungsgemäßen Abwicklung der Aufträge gesetzlich geforderten technischen und organisatorischen Maßnahmen sowie den Schutz der Rechte der betroffenen Personen und wird diese dem Auftraggeber auf Verlangen nachweisen (Art. 28 Abs. 3 lit. h EU-DSGVO). FIO SYSTEMS hat einen Datenschutzbeauftragten bestellt. Die Kontaktdaten des Datenschutzbeauftragen sind unter www.fio.de abrufbar und wurden der Aufsichtsbehörde mitgeteilt (Art. 37 Abs. 7 EU-DSGVO). Dem Auftraggeber und dessen betrieblichen Datenschutzbeauftragten wird das Recht eingeräumt, sich nach Anmeldung grundsätzlich mindestens 5 Tage vorher bei FIO SYSTEMS davon zu überzeugen, dass die vereinbarten Sicherheitsvorkehrungen tatsächlich getroffen wurden (Art. 28 Abs. 3 lit. h EU-DSGVO). FIO SYSTEMS unterrichtet den Auftraggeber unverzüglich bei begründetem Verdacht auf Datenschutzverletzungen und bei Prüfung durch die Aufsichtsbehörde nach Art. 58 EU-DSGVO oder falls eine Aufsichtsbehörde bei FIO SYSTEMS ermittelt (Art. 28 Abs. 3 a.E. EU-DSGVO).

(2) FIO SYSTEMS wird personenbezogene Daten nur gemäß den Weisungen des Auftraggebers verarbeiten (Art. 28 Abs. 3 lit. a EU-DSGVO). Hinsichtlich des Umfangs, der Art und des Zwecks der vorgesehenen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten sowie der Art der Daten und des Kreises der Betroffenen (Art. 28 Abs. 3 EU-DSGVO) gilt Folgendes:

FIO SYSTEMS wird keine personenbezogenen Daten erheben.

FIO SYSTEMS importiert und speichert personenbezogene Daten der Kunden des Auftraggebers entsprechend des Zwecks aus dem geschlossenen übergeordneten Hauptvertrages, dessen Anlage vorliegendes Dokument ist, in einer Datenbank. Die Art der personenbezogenen Daten betrifft personenbezogene Daten der Mitarbeiter des Auftraggebers (z.B. Namen, Zugangsrechte, Kontaktdaten, Systemaktionen, Dokumentenerstellungen, Datenänderungen, Freifeld), der Interessenten des Auftraggebers (z.B. Name, Kontaktdaten, Suchkriterien (Preis, Zimmeranzahl, Lage, Ausstattung), Kaufvertrag, Zahlungseingänge bei Ratenzahlung, Bankverbindung, Freifeld), der Anbieter (z.B. Kontaktdaten, Objektdaten, Bankbindung möglich, Immobilienvermittlungsvertrag, Freifeld), der Auftraggeber und sonstiger Personen (z.B. Kontaktdaten; Bankverbindung; Freifeld).

Eine darüberhinausgehende Nutzung ist nicht zulässig. Der Auftraggeber wird selbst Daten berichtigen, löschen und sperren, soweit keine andere Weisung des Auftraggebers besteht (Art. 28 Abs. 3 e EU-DSVO).

Der Auftraggeber beauftragt FIO SYSTEMS mit der Vornahme aller erforderlichen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 c EU-DSGVO) zur Herbeiführung rationeller Verarbeitung und zur Sicherung der Daten vor Verlust (z. B. Duplizieren von Beständen, Anlegen von Zwischendaten und Arbeitsbereichen etc.), soweit dies nicht zu einer inhaltlichen Umgestaltung der Datei führt.

(3) Die Erhebung, Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland außerhalb des Gebietes des Abkommens über den Europäischen Wirtschaftsraum bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 28 Abs. 3 a und Art. 46 EU-DSGVO erfüllt sind.

(4) FIO SYSTEMS ist verpflichtet, sämtliche FIO SYSTEMS im Zusammenhang mit diesem Vertrag zugänglich werdenden Informationen unbefristet geheim zu halten. FIO SYSTEMS wird seine Mitarbeiter und Dritte, durch die FIO SYSTEMS ggf. Aufträge ausführen lässt, schriftlich (Artikel 28 Abs. 9 EU-DSGVO) auf die Vertraulichkeit sowie auf die Wahrung des Bankgeheimnisses verpflichten bzw. sich ggf. eine Bestätigung geben lassen, dass Dritte ihrerseits bereits ihre Mitarbeiter entsprechend verpflichtet haben (Art. 28 Abs. 3 lit. b EU-DSGVO).

(5) Insbesondere wird FIO SYSTEMS alle in seinem Besitz gelangten Unterlagen des Auftraggebers sorgfältig verwahren und vor Einsichtnahme Unbefugter schützen sowie alle erforderlichen organisatorischen Maßnahmen treffen dass Daten des Auftraggebers gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschung, Diebstahl, widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen und andere unbefugte Bearbeitungen geschützt sind. (Art. 28 Abs. 3 lit. c u i.V.m. Art. 32 EU-DSGVO).

FIO SYSTEMS wird Unterlagen, die Informationen im Sinne von Abs. 3 enthalten, sowie alle vorhandenen Daten des Auftraggebers an den Auftraggeber herausgeben (Art. 28 Abs. 3 lit. g EU-DSGVO), sobald FIO SYSTEMS diese zur Erfüllung der vertraglichen Pflichten nicht mehr benötigt. Die bei der Datenverarbeitung entstandenen Arbeitsdateien und Zwischendateien sind nach Beendigung des Arbeitsablaufes zu löschen, Ausschussmaterial ist sofort datenschutzgerecht zu vernichten, sofern nicht nach geltendem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Artikel 28 Abs. 3 lit. g EU-DSGVO).

Ein Zurückbehaltungsrecht, gleich aus welchem Rechtsgrund, kann insoweit nicht geltend gemacht werden. Vervielfältigungen von Unterlagen im Sinne von Artikel 28 Abs. 3 lit. g sind datenschutzgerecht zu vernichten, sofern der Auftraggeber nicht im Einzelfall eine andere Weisung erteilt.
FIO SYSTEMS stellt dem Auftraggeber vor Löschung und Vernichtung der Daten auf Anfrage des Auftraggebers sowie gegen Zahlung einer entsprechenden Vergütung eine aktuelle Datensicherung zur Verfügung.

(6) FIO SYSTEMS trägt dafür Sorge, dass alle datenschutzrechtlichen Bestimmungen, welche in dem Verantwortungsbereich von FIO SYSTEMS liegen, eingehalten werden. FIO SYSTEMS hat für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten im Rahmen der Auftragsverarbeitung zu sorgen. FIO SYSTEMS ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten oder Unterlagen betroffen sind und wird den Auftraggeber unverzüglich benachrichtigen, sofern Störungen im Rahmen der vertragsgemäßen Bearbeitung der Daten auftreten (Art. 28 Abs. 3 a.E. EU-DSGVO). Zudem wird FIO SYSTEMS den Auftraggeber unverzüglich Anfragen, Beschwerden etc. der Betroffenen an den Auftraggeber weiterleiten. Die Strafbarkeit einer Verletzung der Verpflichtung auf die Vertraulichkeit ist FIO SYSTEMS bekannt.

(7) FIO SYSTEMS setzt zur Erfüllung seiner Verpflichtung als Provider und Subunternehmer PŸUR (ehemals HL komm Telekommunikations GmbH), Nonnenmühlgasse 1, 04107 Leipzig ein.

Ein Wechsel dieses oder sonstiger Subunternehmer darf dann erfolgen, wenn dem kein wichtiger Grund entgegensteht und der Auftraggeber hiergegen keinen Einspruch erhebt (Artikel 28 Abs. 2 S. 2 EU-DSGVO). Ein wichtiger Grund liegt dann vor, wenn Zweifel an der Zuverlässigkeit des neuen Subunternehmers bestehen und/oder die Sicherheit der Daten bei dem neuen Subunternehmer nicht oder nicht in dem nach dieser Vereinbarung geschuldeten Umfang gewährleistet ist. FIO SYSTEMS wird seinem Auftraggeber den Wechsel spätestens 14 Tage im Voraus anzeigen. Die vertraglichen Vereinbarungen zwischen FIO SYSTEMS und den Subunternehmern sind so zu gestalten, dass diese den gesetzlichen und sonstigen rechtlichen Verpflichtungen sowie diesen Vertragsbestimmungen genügen bzw. entsprechen. FIO SYSTEMS erteilt auf schriftliches Verlangen dem Auftraggeber alle erforderlichen Auskünfte (Art. 28 Abs. 4 EUDSGVO).

2. Technische und organisatorische Maßnahmen nach Art. 28 Abs. 3 lit. c i.V.m. Art. 32 EU-DSGVO

A) Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

1. Zutrittskontrolle: Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Der Zugang zum Rechenzentrum in den Räumen der PŸUR wird nur berechtigten Personen gewährt, wenn diese den PIN-Code kennen, eine personalisierte Zutrittskarte besitzen und sich vorher beim RZ-Betreiber angemeldet haben.
- Für das Rechenzentrum sind eine Alarmanlage sowie eine Kameraüberwachung installiert. Die Alarmanlage ist zu einem Wachdienst weitergeschaltet.
- Die Server sind in Schränken im Rechenzentrum verschlossen. Nur befugte Mitarbeiter der FIO SYSTEMS haben Zugang zu den Serverschränken.

- Der Zugang zu den Räumen der FIO SYSTEMS AG ist über personalisierte Transponder am Haupteingang und über Schlüssel zu den Büroräumen abgesichert. Auch das Firmengebäude wird mit einer Alarmanlage und mit Kameras überwacht, ein Wachdienst erhält die Meldungen der Alarmanlage.

2. Zugangskontrolle: Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Die Server sind durch Firewalls geschützt, es werden nur die benötigten Ports freigegeben.
- Der Remotezugriff durch Administratoren der FIO SYSTEMS AG erfolgt ausschließlich verschlüsselt. Für Konten der FIO SYSTEMS AG gelten Passwort-Richtlinien.
- Zugänge zu den Anwendungen sind über vom Kunden anpassbare Passwort-Richtlinien und automatische Sperrung nach mehreren Fehlversuchen geschützt.
- Daten auf mobilen Geräten der FIO SYSTEMS AG werden zusätzlich über Bitlocker-Festplatten-Verschlüsselung geschützt.

3. Zugriffskontrolle: Maßnahmen, um zu 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

- Für Mitarbeiter der FIO SYSTEMS AG werden Zugriffsberechtigungen im 4-Augen-Prinzip vergeben, die aktuellen Berechtigungen werden regelmäßig überprüft.
- Der Datenzugriff der normalen FIO-Benutzer erfolgt durch fein abgestufte Privilegien.
- Zugriffe auf Anwendungen der FIO SYSTEMS AG werden protokolliert, die Logs sind über die Anwendung vom Kunden selbst auswertbar (abhängig von den Berechtigungen des Nutzers)
- Zugriffe auf alle Systeme der FIO SYSTEMS AG werden protokolliert, die Protokolle werden anlassbezogen ausgewertet

4. Trennungsgebot: Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Die verschiedenen FIO-Module speichern ihre Daten in streng getrennten Datenbanken, sofern sie zu unterschiedlichen Zwecken erhoben wurden.

B) Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

1. Weitergabekontrolle: Maßnahmen, um zu 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.

- Datensicherungen, die transportiert werden müssen, werden verschlüsselt, damit bei Verlust kein Einblick möglich ist. Hierbei wird die AES-256-Verschlüsselung genutzt.
- Der Internetverkehr ist zu 100% per SSL verschlüsselt.
- Es wird KEIN drahtloses Netzwerk (WLAN) eingesetzt.

2. Eingabekontrolle: Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Die Remote-Zugriffe werden protokolliert.
- In FIO werden alle Eingabe-, Änderungs- und Löschaktionen protokolliert.

C) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

1. Verfügbarkeitskontrolle: Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Der Serverraum im Rechenzentrum ist stark sauerstoffreduziert, so dass keine Brände entstehen können.
- Eine leistungsfähige Entrauchungsanlage steht zur Verfügung.
- Eine automatisierte Feuermeldeanlage ist vorhanden.
- Die Server sind durch USVs und Notstromaggregate vor Stromausfall und Blitzeinschlag geschützt.
- Die Server sind durch Klimaanlagen vor Überhitzung geschützt.

2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c EU-DSGVO);

- Die verschlüsselten Datensicherungsbänder der wöchentlichen und monatlichen Komplettsicherungen werden regelmäßig von Mitarbeitern der FIO SYSTEMS ausgetauscht, monatlich auf Wiederherstellbarkeit überprüft und anschließend im Bankschließfach gelagert.

D) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)

1. Auftragskontrolle: Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- FIO SYSTEMS setzt zur Erfüllung seiner Verpflichtung als Provider und Subunternehmer die Fa. PŸUR, Leipzig ein. Die vertraglichen Vereinbarungen zwischen der FIO SYSTEMS und dem Subunternehmer bzw. Provider sind so zu gestalten, dass diese den gesetzlichen und sonstigen rechtlichen sowie vertraglichen Verpflichtungen genügen bzw. entsprechen. Es findet keine Auftragsdatenverarbeitung durch PŸUR statt.
- Jeder Mitarbeiter von FIO SYSTEMS hat eine Vereinbarung über den Datenschutz/die Datensicherheit unterschrieben und ist bezüglich Datenschutz/und Datensicherheit geschult worden.

(Anmerkung: Der Vertrag mit PŸUR sieht ein "Server-Housing" vor. Daher hat *PŸUR* keine Zugriffsrechte auf die Server und die Daten. Hier liegt somit keine Auftragsdatenverarbeitung vor. Das Unternehmen *PŸUR* hat einen Datenschutzbeauftragten bestellt.)

Die technisch-organisatorischen Maßnahmen werden laufend durch adäquate Maßnahmen aktualisiert, durch welche das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird.

Die vorstehenden Bestimmungen treten ab dem 25.05.2018 in Kraft.

Leipzig,

_____	_____
Franziska H. Glade, Vorstand	Name Funktion
FIO SYSTEMS AG	Firma