Vereinbarung
für die Verarbeitung von personenbezogenen Daten im Auftrag nach Art. 28 DSGVO

zwischen dem

Auftraggeber oder Verantwortlichen

und

moveIT Software GmbH

(in Folge kurz „**moveIT**")
(Auftragnehmer oder Auftragsverarbeiter)

1. GEGENSTAND UND DAUER DIESER VEREINBARUNG

1.1 Für die Leistungserbringung des zu Grunde liegenden Vertrages mit dem Auftraggeber (z.B. Auftrag über Lizenzen, Dienstleistungsauftrag etc.) verarbeitet der Auftragnehmer personenbezogene Daten („**Daten**") im Auftrag des Auftraggebers als Auftragsverarbeiter im Sinne von Artikel 28 Datenschutz-Grundverordnung (EU) 2016/679 („**DSGVO**").

1.2 Die Laufzeit dieser Vereinbarung beginnt mit Unterzeichnung des zu Grunde liegenden Vertrages des Auftraggebers und endet akzessorisch mit Beendigung oder Kündigung der laufenden Verträge (z.B. Wartungsvertrag über moveIT Lizenzen) und / oder nach Erbringung aller vertraglich vereinbarten Arbeiten.

1.3 Gegenstand der Verarbeitung: **moveIT Lizenzprodukte**

1.4 Art und Zweck der Verarbeitung:

- **Installation und Einrichtung von moveIT Lizenzprodukte im System vom Auftraggeber über Fernwartung**
- **Sonstige Servicearbeiten über Fernwartung in den moveIT Lizenzprodukten im System des Auftraggebers (Konfiguration, Programm- und Stammdatenupdates, Fehlerbehebung)**

2. UMFANG DER AUFTRAGSVERARBEITUNG

2.1 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- **Kunden**
- **Lieferanten**
- **Interessenten**
- **Beschäftigte**
- **Ansprechpartner**

2.2 Art der verarbeiteten Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten:

- **Personenstammdaten** (z.B. Name, Vorname, Geschlecht, Adresse)
- **Angaben zu Ausbildung und Beruf** (z.B. akad. Grad, Berufsbezeichnung)
- **Kommunikationsdaten** (z.B. Telefon, E-Mail)
- **Kundenhistorie** (z.B. Angebote, Aufträge, Reklamationen)

3. PFLICHTEN DES AUFTRAGNEHMERS

3.1 Die Daten werden ausschließlich im Rahmen eines seitens des Auftraggebers erteilten schriftlichen Auftrages – auch in Bezug auf die allfällige Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation - verarbeitet. Diese werden seitens des Auftragnehmers ausschließlich zu dem Zweck verarbeitet, die im Vertrag angegebenen Leistungen zu erbringen. Der Auftragnehmer erlaubt Zugriff auf die Daten nur, soweit dies zur Durchführung des Vertrags erforderlich ist.

3.2 Erhält moveIT einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er, sofern gesetzlich zulässig und sich diese auf einen von ihm erteilten Auftrag beziehen, den Auftraggeber unverzüglich darüber zu informieren und die Aufsichtsbehörde an diesen zu verweisen.

3.3 Der Auftragnehmer darf die Daten, die im Rahmen der Auftragsverarbeitung verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten, wobei weitere Maßnahmen im Umgang mit der betroffenen Person immer dem Auftraggeber obliegen.

3.4 Der Auftragnehmer erklärt gemäß § 6 DSG 2018 rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet und mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht hat. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer unbegrenzt aufrecht.

3.5 Der Auftragnehmer hat den Schutz der Daten durch technische und organisatorische Maßnahmen sicherzustellen, die den Anforderungen von Artikel 32 DSGVO genügen. moveIT hält dabei die im **Anhang** dieser Vereinbarung näher spezifizierten, technischen und organisatorischen Anforderungen ein. Insbesondere ist der Auftragnehmer verpflichtet, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zu unterstützen.

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

3.7 Der Auftragnehmer kann die Maßnahmen in Übereinstimmung mit dem Vertrag erweitern und verbessern. Dies kann zu einer Ablösung bestimmter Maßnahmen durch andere, mindestens genauso effektive Maßnahmen führen, die das gleiche Ziel erreichen. Wesentliche Änderungen sind schriftlich mit dem Auftraggeber zu vereinbaren.

3.8 Wird ein Antrag über Auskunft an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, so leitet der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiter und teilt dies dem Antragsteller mit. Der Auftragnehmer verpflichtet sich, nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen den Auftraggeber dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anfragen betroffener Personen, sofern sich diese auf einen vom Auftraggeber erteilten Auftrag zur Datenverarbeitung seitens des Auftragnehmers beziehen, auf Wahrnehmung der Kapitel III der in der DSGVO genannten Rechte der betroffenen Person nachzukommen.

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

4. WEISUNGSBEFUGNIS UND RECHTE DES AUFTRAGGEBERS

4.1 Der Auftragnehmer wird die Daten ausschließlich nach den dokumentierten Weisungen des Auftraggebers verarbeiten. Sofern eine mündliche Weisung erfolgt, bestätigt der Auftraggeber diese unverzüglich schriftlich. Wenn der Auftragnehmer der Auffassung ist, dass eine Weisung gegen die DSGVO, das DSG 2018 oder andere Datenschutzvorschriften verstößt, wird er den Auftraggeber unverzüglich davon in Kenntnis setzen. Der Auftragnehmer ist nicht verpflichtet, offensichtlich rechtswidrige Weisungen zu befolgen.

4.2 Dem Auftraggeber steht das Recht zu, sich jederzeit, anhand von allen erforderlichen Informationen zum Nachweis der Einhaltung der datenschutzrechtlichen Vorschriften beim Auftragnehmer, zu überzeugen. Der Auftraggeber wird die Auswirkungen der Kontrollen auf den Betrieb des Auftragnehmers so gering wie möglich halten.

5. LÖSCHUNG DER DATEN

5.1 Der Abschluss der vertraglich vereinbarten Arbeiten ist durch eine schriftliche Bestätigung des Auftraggebers festzuhalten. Nach schriftlicher Aufforderung des Auftraggebers, jedenfalls aber nach Beendigung des Auftrags verpflichtet sich der Auftragnehmer, die personenbezogenen Daten nach Wahl des Auftraggebers entweder fachgerecht und vollständig zu löschen oder dem Auftraggeber zurückzugeben. Die Löschung ist dem Auftraggeber schriftlich zu bestätigen.

5.2 Die Pflicht der Löschung gilt nicht, soweit der Auftragnehmer eine gesetzliche Verpflichtung zur Speicherung der entsprechenden personenbezogenen Daten hat. Diese dürfen vom Auftragnehmer dann entsprechend der jeweiligen Aufbewahrungsfristen (insbesondere nach

Handels- oder Steuerrecht) über das Vertragsende hinaus aufbewahrt und erst nach Ablauf der jeweiligen Aufbewahrungsfristen datenschutzgerecht vernichtet werden.

6. UNTERAUFTRAGSVERHÄLTNISSE

6.1 Nimmt der Auftragsverarbeiter zur Verarbeitung eines vom Auftraggeber erteilten Auftrages (im konkreten Einzelfall) einen weiteren Auftragsverarbeiter in Anspruch, so bedarf dies der schriftlichen Genehmigung des Verantwortlichen. Dem weiteren Auftragsverarbeiter werden folglich vertraglich dieselben Datenschutzpflichten auferlegt, die zwischen moveIT und dem Verantwortlichen im Rahmen der Vereinbarung für die Verarbeitung von personenbezogenen Daten im Auftrag nach Art. 28 DSGVO festgelegt wurden.

6.2 Als keine Unterauftragsverhältnisse im Sinne dieser Regelung sind Dienstleistungen wie Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen zu verstehen.

7. SCHLUSSBESTIMMUNGEN

7.1 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des vom Auftraggeber erteilten Auftrages enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

7.2 moveIT hat keinen betrieblichen Datenschutzbeauftragten bestellt. Gemäß Artikel 37 DSGVO ist dies seitens moveIT nicht zwingend erforderlich.

7.3 Die Grundlage für die Anwendung der DSGVO basiert auf österreichischem Recht (DSG 2018). Gerichtsstand ist Wels.

7.4 Diese Vereinbarung ergänzt den Vertrag, auf den sich diese bezieht.

7.5 Sollten Änderungen an dieser Vereinbarung notwendig sein oder werden, um die Voraussetzungen der DSGVO oder der diese ergänzenden oder konkretisierenden nationalen Datenschutzvorschriften zu erfüllen, so verpflichten sich die Parteien diese anzupassen. Eine Änderung, Ergänzung, Aufhebung oder Kündigung dieser Vereinbarung sowie die Änderung dieser Klausel bedarf der Schriftform.

Für den Auftraggeber:	**Für den Auftragnehmer:**
_____	moveIT Software GmbH
Firma	Firma
_____	Wels, 17. Mai 2018
Ort | Datum	Ort | Datum
_____	_____
Unterschrift	Unterschrift
_____	Kevin Hornung, MSc, Verantwortlicher für Datenschutz
Name in Reinschrift	Name in Reinschrift

ANHANG ZUR ANLAGE

Technische und organisatorische Maßnahmen gemäß Artikel 32 (1) DSGVO

1. Gewährleistung der Vertraulichkeit

a) Zutrittskontrolle

Technische bzw. organisatorische Maßnahmen, um einen unbefugten Zutritt zu den Räumlichkeiten, in denen die Daten verarbeitet werden, zu verhindern:

- Besucher werden von der besuchten Person direkt vom Eingangsbereich abgeholt und durch das Haus an die entsprechende Stelle geführt und nach Besuchsende bis zum Ausgang begleitet.
- Der Haupteingang, welcher zu den Geschäftsräumlichkeiten von moveIT führt, ist versperrt, zum Öffnen benötigt man einen Schlüssel. Ausschließlich IT-Personal, welches über einen Schlüssel verfügt, hat Zutritt zu den Severräumlichkeiten. Die Serverräumlichkeiten sind stets versperrt.
- Alarmsicherung von Fenstern und Eingangstüren.

b) Zugangskontrolle

Technische bzw. organisatorische Maßnahmen, um die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern:

- Der Zugang zu den Datenverarbeitungssystemen kann nur mittels einer in der Domäne vergebenen Benutzerkennung und persönlichem Passwort erfolgen.
- Nach fünf fehlerhaften Passworteingaben erfolgt automatisch eine Sperrung der Benutzerkennung. Die Sperre kann nur durch einen Systemadministrator im Rahmen eines definierten Authentifizierungsprozesses aufgehoben werden. Sämtliche Sperrungen von Benutzerkennungen werden protokolliert und vom Systemadministrator regelmäßig kontrolliert.
- Gegen Zugriffe von außen sind die Server durch eine Firewall sowie einem Virenschutz geschützt.

c) Zugriffskontrolle

Technische bzw. organisatorische 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:

- Über die persönliche Mitarbeiterkennung mit dem mitarbeiterindividuellen Passwort erfolgt die Zugriffsregelung über spezielle Programme, mit der jedem/jeder Mitarbeiter/Mitarbeiterin nach seiner/ihrer persönlichen Befugnis Zugriff in die notwendigen Programmabläufe gewährt wird.
- Die Zugriffsberechtigung wird durch Einrichtung einer persönlichen Mitarbeiterkennung hergestellt, welche durch den Systemadministrator vergeben wird.
- Der Systemadministrator kann auf Weisung die Zugriffsmöglichkeit durch Passwortlöschungen oder -änderungen und Prioritätenvergabe kontrollieren.
- Zugriff auf die Serversysteme haben ausschließlich Beschäftigte mit entsprechenden Administrator-Rechten.

- Im Rahmen der Fernwartung wird ein Security Token, falls seitens des Auftraggebers vorhanden, ansonsten ein Fernwartungstool, zur Verbindung in das System des Auftraggebers verwendet. Die Tokens werden versperrt aufbewahrt.

d) Weitergabekontrolle

Technische bzw. organisatorische 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 bzw. stattgefunden hat:

- Die nicht mehr benötigten Datenträger (einschließlich in Papierform) werden von einem qualifizierten Fachbetrieb im Rahmen der Datenschutzbestimmungen physikalisch zerstört und datenschutzgerecht entsorgt.
- Zugriff auf Datenträger ist generell nur Mitarbeitern/Mitarbeiterinnen der IT mit entsprechenden Berechtigungen möglich.
- Bänder mit Sicherungsdateien werden vom System täglich erstellt.
- Sicherungsdatenträger werden extern verwahrt und innerhalb regelmäßigen zeitlichen Abständen gelöscht

2. Gewährleistung der Integrität

a) Eingabe- / Speicherkontrolle

Technische bzw. organisatorische Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, dort verändert oder aus diesen entfernt worden sind:

- Das Löschen gespeicherter Daten ist nur durch einen befugten Personenkreis möglich.

b) Trennungs- bzw. Zweckbindungskontrolle

Technische bzw. organisatorische Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Daten, die für verschiedene Auftraggeber zu unterschiedlichen Zwecken erhoben werden, werden in den Datenbanksystemen von moveIT logisch voneinander getrennt. Das führt dazu, dass die Daten auch nur von den Mitarbeiterinnen und Mitarbeitern gelesen, bearbeitet und verändert werden können, die hierfür die entsprechenden Zugriffsrechte besitzen.

3. Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden technischen bzw. organisatorischen Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Das Gebäude und die IT-Zentrale sind gegen aus einem Blitzschlag resultierenden Schäden abgesichert.

- Die Brandmeldung erfolgt über eine zentrale Brandmeldeanlage, die über einen beauftragten Wachdienst 24 Stunden an 365 Tagen mittelbar mit der Feuerwehr und der Polizei verbunden ist.
- Von den Produktivsystemen werden regelmäßig im Rahmen der Datensicherung Sicherungskopien der Datenbestände erstellt und ausgelagert. Im laufenden Betrieb erfolgt die Speicherung der Daten auf Raid-Systemen oder gespiegelten Datenbanksystemen.
- Feuermelder, USV in IT-Zentrale

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

- Sicherung des CRM-Systems von moveIT 1 x täglich auf virtuellen Rechner, einfache und schnelle Wiederherstellbarkeit durch Bandsicherung
- Interne kundenbezogene Dateiablage mit Zugriffsschutz durch Gruppenrichtlinien wird 1 x täglich gesichert (3-fach-Sicherung): auf zwei verschiedenen virtuellen Servern und auf Band, rasche Wiederherstellbarkeit aufgrund von Snapshot Backups
- Für eine vom Auftraggeber bereitgestellte zentrale Datenablage (z.B. Transfer Cloud) ist der Auftraggeber selbst verantwortlich und haftbar

c) Belastbarkeit

Maßnahmen, die die Belastbarkeit der Systeme und Dienste, die im Zusammenhang mit der Verarbeitung stehen, gewährleisten.

- Alle Datensätze, die im System des Kunden eingepflegt werden, werden bereits bei ihrer Eingabe in die im Hintergrund liegende Datenbank gespeichert (on Demand).

4. Pseudonymisierung und Verschlüsselung

- Der Zugriff außerhalb des Unternehmens auf unsere Datenbanksysteme (CRM, Projekte, Fehler etc.) passiert ausschließlich über eine geschützte VPN-Verbindung. Zusätzlich muss der Benutzer von unserer IT für den VPN-Zugang freigeschaltet werden bevor eine Verbindung möglich ist. Unsere internen Datenbanksysteme sind zusätzlich per Lotus Notes Zertifikat signiert.
- Firmennotebooks sind per Bitlocker (Verschlüsselung der Festplatte) geschützt und sind im Verlust- oder Diebstahlsfall nicht lesbar
- Firmenhandys und Tablets sind im Verlust- oder Diebstahlsfall per Remote sperr- und löschbar
- E-Mails, die innerhalb von moveIT versendet werden, sind standardmäßig verschlüsselt.

5. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Incident-Response-Management
- Mitarbeiterschulungen

- Die Datenbanken im Hintergrund von moveIT@ISS+ sind stets am neuesten Stand der Technik, gewährleistet durch laufende Wartungsverträge mit dem Softwarelieferanten Progress (aktuelle Version Progress 11.7). Alle für moveIT@ISS+ benutzten Frameworks (Windows Komponenten) sind ebenso am neuesten Stand der Technik, ebenso gewährleistet durch laufende Wartungsverträge (Visual C++ 2015 und .Net 4.X). Durch die bei moveIT intern angesiedelte Qualitätssicherung erfolgen in regelmäßigen zeitlichen Abständen Setup Tests.
- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers (Vereinbarung für die Verarbeitung von personenbezogenen Daten im Auftrag nach Art. 28 DSGVO);