Vereinbarung

über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
	IBB Adaptive Solutions GmbH Schönbrunner Straße 218-220, 1120 Wien
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. Präambel

Im Rahmen der Bereitstellung und des Betriebs des Systems Skyline tritt die IBB Adaptive Solutions GmbH im Sinne der EU-DSGVO (EU Datenschutz Grundverordnung) als Auftragsverarbeiter auf. Im Rahmen der Auftragsverarbeitung übernimmt die IBB Adaptive Solutions GmbH die Speicherung der Daten und Bereitstellung des Systems Skyline zum Zugriff auf die gespeicherten Daten.
Die IBB Adaptive Solutions GmbH stellt dabei sicher:

- Daten werden nicht an Dritte zur Nutzung weitergegeben
- Daten werden bei Löschung vollständig aus den Systemen gelöscht
- Daten werden nicht in Drittsysteme oder für andere Verarbeitungszwecke übernommen
- Daten werden nach aktuellem Stand der Technik vor Verlust geschützt
    - Es werden regelmäßige Backups angefertigt. Diese werden in unterschiedlichen, geografisch getrennten Rechenzentren aufbewahrt
- Daten werden nach dem aktuellen Stand der Technik gegen unbefugten Zugriff geschützt
    - Die Infrastruktur ist vor physischem Zugriff in Rechenzentren geschützt
    - Die Betriebssysteme werden auf aktuellstem Stand im Hinblick auf Updates gehalten
    - Systemkomponenten, welche dies nicht erfordern, sind nicht auf öffentlichen Netzen zugänglich
    - Passwörter für administrative Zugänge werden restriktiv vergeben und entsprechen ein Passwort-Policy nach aktuellem Stand der Technik
- Daten werden ausschließlich innerhalb der EU bzw. in einem Staat verarbeitet, der ein angemessenes Datenschutzniveau aufweist (nach vorliegendem Angemessenheitsbeschluss der Europäischen Kommission)

In Hinblick auf die DSGVO und die lokalen Datenschutzgesetzte, muss der Anwender bzw. der Administrator des Kunden sicherstellen,

- dass er das Einverständnis der betroffenen Personen zur Speicherung und Verarbeitung der Daten eingeholt hat
- dass er für die Aktualität der gespeicherten personenbezogenen Daten sorgt
- dass er den Auskunftsrechten der betroffenen Personen nachkommt
- dass er Datensätze nach den Anforderungen der DSGVO im System löscht
- dass er Daten nicht unberechtigt vermarktet oder an Dritte weitergibt
- dass er keinen unbefugten Personen Zugang zum System Skyline gewährt
- dass inaktive Nutzerkonten im System deaktiviert werden
- dass er sicherstellt, dass alle Anwender sichere Passwörter nach aktuellem Stand der Technik wählen

2. Gegenstand der Vereinbarung

(1) Gegenstand

Der Gegenstand dieses Auftrages ist die Bereitstellung der Software-Lösung „Skyline“ sowie alle damit verbundenen Tätigkeiten wie Wartung und Support.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Unternehmensstammdaten
- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Nachrichten
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Ansprechpartner

3. Dauer der Vereinbarung

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist lt. Vertrag gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

4. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, personenbezogene Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der zur Ausführung der Hosting- und Wartungsleistungen für die Software „Skyline“ erforderlichen Tätigkeiten zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

(3) Wahrung der Vertraulichkeit und Verschwiegenheit: Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor

Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(4) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).

(5) Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.
Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(6) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben oder in dessen Auftrag zu vernichten. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

5. Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.
Einzelheiten sind dem Anhang zu entnehmen.

6. Ort der Durchführung der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt primär innerhalb der EU bzw. des EWR.
Sofern personenbezogene Daten auch außerhalb der EU bzw. des EWR verarbeitet bzw. gespeichert werden, so erfolgt dies ausschließlich in Staaten welche ein angemessenes Datenschutzniveau aufweisen. Das angemessene Datenschutzniveau ergibt sich aus:

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO
- einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO

7. Sub-Auftragsverarbeiter

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden.
  Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

_____, am _____	_____, am _____
Für den Auftraggeber:	Für den Auftragnehmer:
.....	.....

Anhang – Technisch-organisatorische Maßnahmen (TOMs)

VERTRAULICHKEIT

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.

INTEGRITÄT

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Backup-Strategie (online/offline; on-site/off-site);
- Rasche **Wiederherstellbarkeit**.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen.