Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
	bbit GmbH **Erzherzog-Karl-Straße 252/9+10** **1220 Wien**
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

Bilanzbuchhaltung / Personalverrechnung / IT-Dienstleistung

(2) Diese Vereinbarung ist als Ergänzung zur erteilten Vollmacht zu verstehen.

(3) Rechtsgrundlage:
Zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich (Art. 6 Abs. 1 Lit c)
Einwilligung (Art. 9 Abs. 2 lit. a)
Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen
Zur Vertragserfüllung notwendig (Art. 6 Abs. 1 lit. b)

(4) Folgende Datenkategorien von betroffenen Personen werden verarbeitet:

Personalverrechnung:
Die beim Verantwortlichen angestellten Mitarbeiter werden aufgrund einer Meldung des Verantwortlichen zum Zwecke der Personalverwaltung in einer Personaldatenbank erfasst. In der Personaldatenbank sind neben persönlichen Verwaltungsdaten des Mitarbeiters unter anderem Daten zur Qualifikation, sonstigen Kompetenzen sowie Abrechnungsdaten (Arbeitszeit, Urlaubs-, Krankenstandstage) von Mitarbeitern gespeichert. Dies dient vor allem der Personalplanung und -entwicklung (Einsatz des Mitarbeiters an einer passenden Arbeitsstelle, Planung des zukünftigen Personalbedarfs, Notwendigkeit der Einstellung neuer Mitarbeiter, ...).
Die in der Mitarbeiterdatenbank gespeicherten Daten können auch sensible Daten im Sinne des Art. 9 DSGVO umfassen, nämlich das Religionsbekenntnis (im Falle der freiwilligen Angabe des Mitarbeiters, etwa um in den Genuss religionsspezifischer gesetzlicher Feiertage zu kommen), Gesundheitsdaten (gegebenenfalls bestehende Behinderungen oder andere gesundheitliche Beeinträchtigungen von Mitarbeitern, um bei der Gestaltung des Arbeitsverhältnisses darauf Rücksicht nehmen zu können) oder eine etwaige Gewerkschaftszugehörigkeit (wenn der Mitarbeiter den Gewerkschaftsbeitrag über die Lohnverrechnung abrechnen lassen möchte). Auch die Sozialversicherungsnummer, die möglicherweise als sensibles Datum zu qualifizieren ist, wird zum Zwecke der Lohnverrechnung in die Mitarbeiterdatenbank aufgenommen.
Die Personaldatenbank enthält zudem die Kontaktdaten von Lebenspartnern und Kindern um steuer- und sozialversicherungsrechtliche Begünstigungen anwenden zu können.

Die Daten ehemaliger Mitarbeiter werden nur so lange aufbewahrt, als dies gesetzlich vorgeschrieben ist. Die buchhaltungsrelevanten Arbeitnehmerdaten (zur Lohnverrechnung notwendig) werden dem § 132 BAO entsprechend nach 7 Jahren gelöscht. Der Name, die Anschrift, der Zeitraum der Anstellung und die vom Mitarbeiter ausgeführten Tätigkeiten werden zur Erfüllung des Anspruches auf ein Dienstzeugnis für 30 Jahre gespeichert, sofern ein solches Dienstzeugnis nicht schon zuvor rechtmäßig ausgestellt wurde.
Elektronisch abgelegte Daten sind vor Fremdzugriff geschützt und zur Sicherung der Richtigkeit und Vollständigkeit der Datensätze wird ein regelmäßiges Back-Up durch-geführt.

Rechtsgrundlage Ergänzung für den Bereich Personalverrechnung:
Nicht-sensible Daten:

- Zur Vertragserfüllung notwendig: Kontaktdaten, buchhaltungsrelevante Daten, Daten für das Dienstzeugnis
- Zur Erfüllung einer rechtlichen Verpflichtung: lohnsteuer- und sozialversicherungs-relevante Daten (Arbeitszeit, Urlaubs-, Krankenstandstage)
- Zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten: Daten naher Angehöriger

Sensible Daten:

- Mit Einwilligung nach Art. 9 Abs. 2 lit a.): Gewerkschaftszugehörigkeit, religiöses Bekenntnis
- Zur Erfüllung einer aus dem Arbeitsrecht oder dem Recht auf soziale Sicherheit entspringenden Verpflichtung nach Art. 9 Abs.2 lit b.): Behinderung, SV-Nummer

Bilanzbuchhaltung

Die dem Verantwortlichen bekanntgegebenen Daten von Kunden und Lieferanten (inklusive der Kontaktdaten der jeweiligen Unternehmen und Personen) werden in einer Finanzbuchhaltungs-Datenbank erfasst. Die Datenbank enthält neben den Namen und Kontaktdaten der Unternehmen auch Daten über entsprechende Geschäftsfälle, Zahlungsmodalitäten und Offene Posten.
Die Daten werden nur so lange aufbewahrt, als dies gesetzlich vorgeschrieben ist. Die buchhaltungsrelevanten Daten werden dem § 132 BAO entsprechend nach 7 Jahren gelöscht.
Daten, die zur Geltendmachung, Ausübung oder Verteidigung von vertraglichen Ansprüchen erforderlich sind, werden entsprechend den gesetzlichen Verjährungsfristen bis zu einer Dauer von drei Jahren ab Beendigung des Vertragsverhältnisses gespeichert.
Sonstige Speicherdauern können sich insbesondere aus anderweitigen gesetzlichen Aufbewahrungsfristen ergeben.
Elektronisch abgelegte Daten sind vor Fremdzugriff geschützt und zur Sicherung der Richtigkeit und Vollständigkeit der Datensätze wird ein regelmäßiges Back-Up durch-geführt

2. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von drei Monaten zum Ende eines Kalendermonats gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. 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. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) 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 Verschwiegenheitsverpflichtungen unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person 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. 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.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (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).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(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, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten[1]. Auf das gesetzliche Zurückbehaltungsrecht (§ 471 ABGB, § 369 UGB) wird in diesem Zusammenhang verwiesen.

(9) Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(10) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

[1] Nichtzutreffendes bitte streichen.

4. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

5. Sub-Auftragsverarbeiter

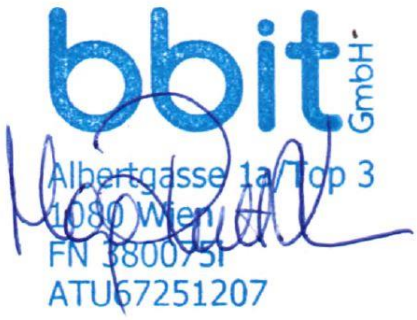
Der Auftragnehmer kann Sub-Auftragsverarbeiter hinzuziehen.
Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. 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.

Wien am

…….

Für den Auftraggeber:

Für den Auftragnehmer:



……
[*Name samt Funktion*]

……
Mag. Ruth KORPER (GF)]

Anlage – Technisch-organisatorische Maßnahmen des Auftragsverarbeiters

VERTRAULICHKEIT

- **Zutrittskontrolle:** erfolgt über eine Alarmanlage mit Chipkarten und elektrische Türöffner
- **Zugangskontrolle**: In den Büroräumen sind ausschließlich Net-Clients eingerichtet, die nur über die Eingabe von Benutzernamen und Passwort die Verbindung zur Workstation ermöglichen. Die Kennwörter werden alle 4 Monate zwingend verändert. Es müssen Komplexe Passwörter sein. Über Dateirechte ist gewährleistet, dass, nur die User der entsprechenden Abteilung die Daten einsehen und verändern können.
- **Zugriffskontrolle**: Die Net-Clients haben keine Möglichkeit Daten per USB auszutauschen. Ein USB-Server stellt sicher, dass ein Datenaustausch nur über authentifizierte Benutzer erfolgen kann.
- **Pseudonymisierung und Verschlüsselung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt. Sofern für die jeweilige Datenverarbeitung möglich, werden folgende Verschlüsselungstechnologien eingesetzt: SSH, TLS
- **Klassifikationsschema für Daten:** intern

INTEGRITÄT

- **Weitergabekontrolle**: Die Datenübertragung zu den Mail-Clients erfolgt mittels SSH-Verschlüsselung. Die Verbindung der Remotebenutzer ist TLS verschlüsselt. Die Übertragung nach außen ist nur über Virtual Private Networks (VPN) möglich. Der Datenaustausch mit Kunden erfolgt über ein personalisiertes Kundenportal.
- **Eingabekontrolle**: Die Eingabekontrolle erfolgt über die Systemlogs der Software und das hauseigenen Dokumentenmanagement. Jeder Dateizugriff wird protokoliert und mit Benutzernamen abgespeichert.

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Es ist eine Hardwarefirewall eingerichtet, die den Zugriff vom Internet in ein eigenes Subnet legt. Von diesem Subnet sind keinerlei Dateizugriffe zugelassen. Ein zentralverwalteter Virenscann ist installiert, zusätzlich werden die Mails vorab am Mailserver auf Viren geprüft. Die Sicherungen werden von einem eigenen Sicherungsserver erstellt. Damit ist gewährleistet, dass die Sicherungslaufwerke nicht permanent gemountet sind. Es lauft eine tägliche Inkrementelle/differenzielle Sicherung und wöchentlich eine Vollsicherung auf 4 unterschiedlichen Festplatten, die nur für Sicherungen verwendet werden. Die Datenträger werden im Rad überschrieben und sind 4 Wochen gültig. Zusätzlich werden die wöchentlichen Vollsicherungen auch auf Wechseldatenträgern kopiert.
- **Löschungsfristen**: Die Daten werden nur so lange aufbewahrt, als dies gesetzlich vorgeschrieben ist. Die buchhaltungsrelevanten Daten werden dem § 132 BAO entsprechend nach 7 Jahren gelöscht. Daten, die zur Geltendmachung, Ausübung oder Verteidigung von vertraglichen Ansprüchen erforderlich sind, werden entsprechend den gesetzlichen Verjährungsfirsten bis zu einer Dauer von drei Jahren ab Beendigung des Vertragsverhältnisses gespeichert. Sonstige Speicherdauern können sich insbesondere aus anderweitigen gesetzlichen Aufbewahrungsfristen ergeben. Log-Files, etc. werden mit Ablauf der allgemeinen Verjährungsfrist gelöscht.

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- **Überprüfung:** Einmal jährlich werden alle Maßnahmen überprüft und nötigenfalls angepasst. Der berechtigte Personenkreis wird einmal jährlich auf Einhaltung geschult.
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung oder Zustimmung des Auftraggebers.