Auftragsverarbeitungsvertrag

nach Art 28 DSGVO

abgeschlossen zwischen

dem Verantwortlichen der Firma

_____

einerseits

und

Benefit Büroservice GmbH

Europaplatz 5

3100 St. Pölten

nachstehend „Auftragsverarbeiter“ genannt

andererseits

wie folgt:

Auftragsverarbeitungsvertrag
Stand 01.06.2024

Präambel

Diese Vereinbarung ist als Ergänzung zu den bestehenden Verträgen zwischen Verantwortlicher und Auftragsverarbeiter zu verstehen.

Sie konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den bestehenden Verträgen zu ihrer in Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit den bestehenden Verträgen in Zusammenhang stehen und bei denen Beschäftige des Auftragsverarbeiters oder durch den Auftragverarbeiters Beauftragte, personenbezogene Daten des Verantwortlichen verarbeiten.

1. Gegenstand der Vereinbarung

1.1. Aus den bestehenden Verträgen ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

1.2. Folgende Arten von personenbezogenen Daten werden zum Zweck der Vertragserfüllung und der Dokumentation verarbeitet:

- Daten vom Verantwortlichen: Logindaten [Benutzername, Passwort], Stammdaten Kontaktdaten [Name, Adresse, Emailadresse, Telefonnummer, etc.], Firmendaten [Firmenname, UID, Rechtsform, etc.], Bankdaten [Bank, IBAN, BIC, Kontoinhaber], Ansprechpersonen vom Unternehmen [Name, Titel, Emailadresse, Telefonnummer, Zuständigkeit, Status], Kommunikationsinhalte, individuell definierte Daten
- Daten für den Auftragsverarbeiter: Kontaktdaten, Firmendaten, Kommunikationsinhalte, individuell definierte Daten
  Die Datenverarbeitung kann je nach Kunden und gebuchter Leistungen/Optionen variieren.

1.3. Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

Kunden, Interessenten, Lieferanten, Mitarbeiter, Geschäftspartner, Anrufer

1.4. Die Verarbeitung ist folgender Art:

- Daten des Verantwortlichen: Zur Vertragserfüllung werden die vom Verantwortlichen mitgeteilten Daten erfasst, verarbeitet und gespeichert.
- Daten für den Auftragsverarbeiter: Für den Verantwortlichen werden die Daten, die im Zuge des Telefonats mitgeteilt werden, mittels einer Anrufinformation erfasst, gespeichert, verarbeitet und an den Verantwortlichen übermittelt.

2. Dauer der Vereinbarung

2.1. Dieser Vertrag beginnt mit einer schriftlichen Bestätigung per E-Mail über die Einrichtung der Dienste und Zielrufnummern.

2.2. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des jeweiligen bestehenden Vertrags, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

2.3. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt von Punkt 2.2. unberührt.

3. Anwendungsbereich und Verantwortlichkeit

3.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Dies umfasst Tätigkeiten, die in den bestehenden Verträgen konkretisiert sind. Der Auftraggeber ist im Rahmen der bestehenden Verträge für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich. („Verantwortlicher“ im Sinne des Art. 4 Z 7 DSGVO).

4. Pflichten und Rechte des Auftragsverarbeiters

4.1. Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen – zu verarbeiten, sofern er nicht hierzu rechtlich verpflichtet ist. In solch einem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern eine solche Mitteilung nicht rechtlich verboten ist.

4.2. Der Auftragsverarbeiter 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 Auftragsverarbeiter aufrecht.

4.3. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1[1] zu entnehmen).

4.4. Der Auftragsverarbeiter ergreift technische und organisatorische Maßnahmen, damit der Verantwortliche seine Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person (zB Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller mitzuteilen.

4.5. Der Auftragsverarbeiter unterstützt unter Berücksichtigung der Art der Vereinbarung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (zB 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).

4.6. Der Auftragsverarbeiter hat für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 30 DSGVO zu erstellen.

4.7. Dem Verantwortlichen 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 Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

4.8. Kontrollen oder Einsichtnahme beim Auftragsverarbeiter haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Verantwortlichen zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragsverarbeiters sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragsverarbeiter den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle nach Stichproben oder Dokumentation erfolgen.

4.9. Der Auftragsverarbeiter ist nach Beendigung dieser Vereinbarung verpflichtet – sofern nicht eine rechtliche Verpflichtung zur Speicherung besteht bzw. vertraglich konkrete Fristen zur Speicherung vereinbarten wurden– alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Verantwortlichen in einem angemessenen Zeitraum zu übergeben bzw. in dessen Auftrag zu vernichten.

4.10. Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung des Verantwortlichen durchführen.

[1] Anlage 1 (technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO)

5. Pflichten des Verantwortlichen

5.1. Der Verantwortliche sichert dem Auftragsverarbeiter zu, die von ihm bereit gestellten personenbezogenen Daten im Einklang mit den jeweils gültigen datenschutzrechtlichen Bestimmungen zu verarbeiten und zur Datenverarbeitung berechtigt zu sein.

5.2. Der Verantwortliche erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen hat der Verantwortliche jedoch unverzüglich dokumentiert zu bestätigen.

5.3. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

5.4. Der Verantwortliche verpflichtet sich, die Stammdaten, Bankdaten sowie alle weiteren angegebenen Informationen im benefit Kundenportal aktuell zu halten.

5.5. Der Verantwortliche trägt selbst die Verantwortung für die Sicherheit der benefit Kundenportal Logindaten, indem er die Zugangsdaten – insbesondere das Passwort – sicher verwahrt und regelmäßig ändert.

6. Ort der Durchführung der Datenverarbeitung

6.1. Alle Datenverarbeitungstätigkeiten seitens des Auftragsverarbeiters werden nach Möglichkeit nur innerhalb der EU durchgeführt. Diverse Dienste, die seitens des Auftragsverarbeiters genutzt werden, werden allerdings auch zu Datenspeicherungen außerhalb der EU führen. Der Auftragsverarbeiter wird nur Unternehmen auswählen, die die Regelungen nach der DSGVO anwenden und das erforderliche Schutzniveau gegenüber dem Auftragsverarbeiter einhalten und diese Einhaltung auch ihm gegenüber bestätigen.

7. Sub-Auftragsverarbeiter

7.1. Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter für folgende Tätigkeiten hinzuziehen:

- IT
- Telefonanlage
- Reporting
- Kalender
- Telefonannahme
- Email Bearbeitung
- Zurverfügungstellung von Telefonnummern
- Rechnungsdruck und Briefversand
- Buchhaltung
- Steuerberatung
- Inkasso
- Geschäftsadressen

7.2. Der Verantwortliche kann vom Auftragsverarbeiter jederzeit eine Auflistung der einzelnen Sub-Auftragsverarbeiter anfordern. Der Auftragsverarbeiter schließt den erforderlichen Vertrag 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 Auftragsverarbeiter auf Grund dieses Vertrages obliegen.

8. Technische und organisatorische Maßnahmen

8.1. Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 DSGVO zu berücksichtigen (Einzelheiten in Anlage 1[2]).

8.2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen.

8.3. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und zuvor dem Verantwortlichen mitzuteilen.

9. Berichtigung, Einschränkung und Löschung von Daten

9.1. Der Auftragsverarbeiter darf die Daten, die aufgrund dieses Vertrages verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

9.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenübertragbarkeit und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

10. Haftung und Schadenersatz

10.1. Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelungen.

[2] Anlage 1 (technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO)

11. Sonstiges

11.1. Die zuständige Aufsichtsbehörde ist die österreichische Datenschutzbehörde.

11.2. Soweit Handlungen in dokumentierter Form zu erfolgen haben, ist damit die schriftliche Durchführung der Handlung gemeint; E-Mail genügt diesem Schriftlichkeitserfordernis.

11.3. Änderungen und Ergänzungen dieses Vertrages – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – 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.

11.4. Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt.

11.5. Es gilt österreichisches Recht.

11.6. Alle Streitigkeiten, die sich aus diesem Vertrag ergeben, werden durch das für 3100 St. Pölten sachlich zuständige staatliche Gericht entschieden.

St. Pölten	Ort Datum
Für den Auftragsverarbeiter	Für den Verantwortlichen
_____	_____
Barbara Brandstetter, Geschäftsführerin	Name: Firma: Funktion:

Anlage 1

Anlage 1 - Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen		
Maßnahmen laut Art. 32	**Sicherheitsmaßnahme**	**Umsetzung**
Vertraulichkeit	**Zutrittskontrolle** (Schutz vor unbefugten Zutritt)	Zutritt zu den Büroräumen nur durch oder in Begleitung von berechtigten Personen; Alle Mitarbeiter besitzen Chipkarten; Der Eingang ist außerdem durch einen Empfang zu den Bürozeiten besetzt; elektrischer Türöffner und Videoüberwachung sind vorhanden; Akten in versperrbaren Schränken; Server befindet sich getrennt von herkömmlichen Büroräumen und sind gesondert zutrittsgeschützt (verschlossener Raum, kontrollierte Schlüsselausgabe); eigene Besprechungszimmer in denen keine Akten zugänglich sind; Server befinden sich außerdem in Rechenzentren mit Standort im EU Raum
	Zugangskontrolle (Schutz vor unbefugter Systembenutzung)	sichere Kennwörter; automatische Sperrmechanismen; persönlicher Benutzerlogin pro Mitarbeiter; Firewall; Verpflichtung aller Mitarbeiter auf das Datengeheimnis und Telekommunikationsgeheimnis
	Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)	Unterschiedliche Zugriffsberechtigungen; teilweise Protokollierung der Zugriffe; periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten; sichere Aufbewahrung von Speichermedien; datenschutzgerechte Entsorgung von Geräten mit Speichermedien; datenschutzgerechtes Löschen und Wiederverwenden von Speichermedien (Sticks); Bildschirm- und Computersperre bei Verlassen des Arbeitsplatzes
Integrität	**Weitergabekontrolle** (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)	Daten werden nur an berechtigte Empfänger übermittelt; VPN bzw. Verschlüsselung von Datenträgern
	Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)	Teilweise Protokollierung von Zugriffen; relevante Nutzeraktivitäten werden protokolliert; für jeden Mitarbeiter ein eigener Zugang mit Zufgriffberechtigungen nach Aufgabengebiet (Rechtemanagement)
Verfügbarkeit und Belastbarkeit	**Verfügbarkeitskontrolle** (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)	Backup-Strategie; Spiegelung von Festplatten (RAID); Klimaanlage im Serverraum und unterbrecherungsfreie Stromversorgung (USV); Brandmeldeanlage; Brandschutzmaßnahmen im Serverraum und Büros; laufende Updates; Virenschutz; Firewall
Pseudonymisierung und Verschlüsselung	**Pseudonymisierung**	Sofern für die jeweilige Datenverarbeitung möglich und sinnvoll, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt (z.B. IP-Adressen, Anonymisierung in Google Analytics)
	Verschlüsselung	Sofern für die jeweilige Datenverarbeitung möglich, werden Verschlüsselungstechnoligien eingesetzt (z.B. Verwenden von Verschlüsselten USB Sticks)
Evaluierungsmaßnahmen	**Datenschutz-Management**	Verarbeitungsverzeichnis aktuell halten; regelmäßiger Mitarbeiter-Schulungen