Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

zwischen
dem Auftraggeber (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO)
– im Folgenden „Verantwortlicher“ oder „Auftraggeber“ –

und

BetterBenefit GmbH (Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO)
– im Folgenden „Auftragsverarbeiter“ –

Präambel

Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Rahmen der Zusammenarbeit.
Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Auftrag und auf dokumentierte Weisung des Auftraggebers gemäß Art. 28 DSGVO.
Beide Parteien verpflichten sich zur Einhaltung der geltenden Datenschutzvorschriften, insbesondere der Datenschutz-Grundverordnung (DSGVO).

Diese Vereinbarung wird Bestandteil des Maklermandats und bedarf keiner gesonderten Unterzeichnung.

---

1. Gegenstand und Dauer der Verarbeitung

(1) Der Auftragsverarbeiter erbringt Unterstützungsleistungen bei der Beratung, Betreuung und Administration betrieblicher Vorsorgelösungen, insbesondere betrieblicher Altersvorsorge, betrieblicher Krankenversicherung, Zeitwertkonten und Berufsunfähigkeitsabsicherung.

(2) Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zur Erfüllung dieser Aufgaben und nur auf Weisung des Auftraggebers.

(3) Die Verarbeitung beginnt mit Abschluss des Hauptvertrags und endet mit Beendigung des Mandats sowie vollständiger Rückgabe oder Löschung der Daten.

(4) Gesetzliche Aufbewahrungspflichten bleiben unberührt.

2. Art der verarbeiteten Daten und betroffene Personen

(1) Kategorien der verarbeiteten Daten:

- Personalstammdaten (Name, Adresse, Geburtsdatum, Sozialversicherungsnummer)
- Vertrags- und Leistungsdaten
- Einkommens- und Steuerdaten
- Bankverbindungsdaten
- Gesundheitsdaten (nur mit ausdrücklicher Einwilligung)

(2) Betroffene Personengruppen:

- Mitarbeitende des Auftraggebers
- Ehemalige Mitarbeitende und Versorgungsempfänger

---

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist allein verantwortlich für die Rechtmäßigkeit der Datenverarbeitung.

(2) Der Auftraggeber informiert die betroffenen Personen gemäß Art. 13 DSGVO und holt erforderliche Einwilligungen ein.

(3) Der Auftraggeber führt erforderliche Datenschutz-Folgenabschätzungen eigenverantwortlich durch.

(4) Der Auftraggeber kann Weisungen hinsichtlich Art, Umfang und Mitteln der Verarbeitung jederzeit in Textform erteilen.

(5) Der Auftraggeber benennt eine weisungsberechtigte Kontaktperson gegenüber dem Auftragsverarbeiter.

---

4. Pflichten des Auftragsverarbeiters

(1) Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung des Auftraggebers.

(2) Verpflichtung aller Mitarbeiter und etwaiger Subunternehmer zur Vertraulichkeit.

(3) Umsetzung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO.

(4) Unverzügliche Information bei Datenschutzverletzungen oder Rechtsverstößen.

(5) Unterstützung des Auftraggebers bei der Wahrnehmung von Betroffenenrechten und Meldepflichten (nur im Rahmen der Möglichkeiten und auf Weisung).

(6) Führung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO.

(7) Nach Beendigung des Auftrags wird der Auftragsverarbeiter die personenbezogenen Daten entweder auf Weisung des Auftraggebers datenschutzkonform löschen oder diesem zurückgeben, soweit dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Erfolgt keine Weisung innerhalb angemessener Frist, erfolgt die datenschutzkonforme Löschung.

---

5. Einsatz von Subunternehmern

(1) Der Auftraggeber kann der Einbindung eines neuen Subunternehmers innerhalb von 14 Tagen aus wichtigem Grund widersprechen.

(2) Alle Subunternehmer werden vertraglich DSGVO-konform eingebunden.

(3) Eine aktuelle Liste der Subunternehmer wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

---

6. Technische und organisatorische Maßnahmen (TOMs)

(1) Der Auftragsverarbeiter trifft angemessene Maßnahmen, insbesondere:

- Zutritts-, Zugangs- und Zugriffskontrollen

- Verschlüsselung von Datenübertragungen
- Berechtigungsmanagement und Rollenkonzepte
- Protokollierung von Zugriffen und Änderungen
- Verfügbarkeits- und Wiederherstellungskonzepte
- Schulungen der Beschäftigten zum Datenschutz

(2) Aktualisierte TOMs werden dem Auftraggeber auf Anfrage zur Verfügung gestellt.

---

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Anforderungen beim Auftragsverarbeiter zu prüfen.

(2) Der Auftragsverarbeiter unterstützt diese Kontrollen durch Vorlage geeigneter Nachweise (z. B. Zertifikate, Auditberichte).

(3) Vor-Ort-Kontrollen erfolgen nach vorheriger Ankündigung und unter Wahrung der Vertraulichkeit und Betriebsabläufe.

---

8. Vertragsbeendigung

(1) Nach Beendigung der Verarbeitung sind alle personenbezogenen Daten auf Weisung zu löschen oder zurückzugeben.

(2) Der Auftragsverarbeiter dokumentiert die Löschung.

(3) Ein Zurückbehaltungsrecht an den Daten wird ausgeschlossen.

---

9. Schlussbestimmungen

(1) Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Textform.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, bleibt die Wirksamkeit im Übrigen unberührt.

(3) Diese Vereinbarung wird Bestandteil des Maklermandats und bedarf keiner gesonderten Unterzeichnung.

(4) Es gilt ausschließlich deutsches Recht. Gerichtsstand ist der Sitz des Auftragsverarbeiters.

Stand: 01.01.2025