

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Muster-Fassung · Stand Juli 2026

zwischen

[Name / Firma des Auftraggebers], [Anschrift]

– nachfolgend „Auftraggeber“ –

und

Dr. rer. medic. Franz Hütter, M.A., BRAIN-HR, Am Schlagbaum 1, 58285 Gevelsberg

– nachfolgend „Auftragnehmer“ –

§ 1 Gegenstand und Dauer der Verarbeitung

Der Auftragnehmer erbringt für den Auftraggeber Leistungen der wissenschaftlichen Evaluation und Wirkungsmessung von Weiterbildungs- und Entwicklungsmaßnahmen (insbesondere Konzeption, Durchführung und Auswertung von Befragungen und Erhebungen über die Plattform studies.brain-hr.com sowie zugehörige Beratungsleistungen) gemäß dem zugrunde liegenden Hauptvertrag. Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung

Erhebung, Speicherung, Auswertung und pseudonymisierte bzw. aggregierte Berichtslegung von Befragungs- und Testdaten zum Zweck der Evaluation von Lern- und Entwicklungsmaßnahmen des Auftraggebers. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt.

§ 3 Art der personenbezogenen Daten

- Stamm- und Kontaktdaten (z. B. Name, dienstliche E-Mail-Adresse), soweit für Einladungs- und Teilnahmemanagement erforderlich
- Befragungs- und Antwortdaten (Selbstauskünfte, Einschätzungen, Testwerte)
- Meta- und Nutzungsdaten der Erhebungsplattform (z. B. Zeitstempel der Teilnahme)

Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) sind nicht Gegenstand des Auftrags, sofern nicht im Einzelfall gesondert schriftlich vereinbart.

§ 4 Kategorien betroffener Personen

- Beschäftigte des Auftraggebers
- Teilnehmende an Weiterbildungs-, Trainings- und Entwicklungsmaßnahmen des Auftraggebers

§ 5 Pflichten des Auftragnehmers

- Verarbeitung ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DS-GVO)
- Verpflichtung aller mit der Verarbeitung befassten Personen auf Vertraulichkeit (lit. b)

- Umsetzung der technischen und organisatorischen Maßnahmen nach Anlage 2 (lit. c, Art. 32 DS-GVO)
- Unterstützung des Auftraggebers bei Betroffenenrechten sowie bei Pflichten nach Art. 32 bis 36 DS-GVO (lit. e, f)
- Löschung oder Rückgabe aller personenbezogenen Daten nach Auftragsende nach Wahl des Auftraggebers (lit. g)
- Bereitstellung aller erforderlichen Informationen zum Nachweis der Pflichten sowie Ermöglichung und Duldung von Überprüfungen (lit. h)
- Unverzügliche Information des Auftraggebers, wenn eine Weisung nach Auffassung des Auftragnehmers gegen Datenschutzrecht verstößt

§ 6 Weisungsrecht des Auftraggebers

Weisungen erfolgen in Textform. Weisungsberechtigte und -empfangende Personen werden im Hauptvertrag oder gesondert benannt.

§ 7 Subauftragsverarbeiter

Der Auftraggeber erteilt die allgemeine Genehmigung zur Einschaltung der nachfolgenden Subauftragsverarbeiter. Der Auftragnehmer informiert über beabsichtigte Änderungen; der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland – Server-Hosting (Rechenzentrum in Deutschland, ISO-27001-zertifiziert, TÜV-Rheinland-geprüfte Rechenzentrums-Maßnahmen). Mit dem Anbieter besteht eine Vereinbarung zur Auftragsverarbeitung.

Eine Verarbeitung in Drittländern außerhalb der EU/des EWR findet nicht statt.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, und unterstützt bei der Erfüllung der Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DS-GVO.

§ 9 Löschung und Rückgabe

Nach Abschluss des Auftrags löscht der Auftragnehmer sämtliche personenbezogenen Daten datenschutzgerecht oder gibt sie zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Löschung wird auf Verlangen schriftlich bestätigt. Aggregierte, nicht personenbeziehbare Auswertungsergebnisse bleiben hiervon unberührt.

§ 10 Nachweis und Kontrollen

Der Auftraggeber kann sich vor Beginn und während der Verarbeitung von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen, in der Regel durch Einholung von Selbstauskünften oder geeigneten Nachweisen; Vor-Ort-Kontrollen erfolgen nach Ankündigung mit angemessener Frist zu üblichen Geschäftszeiten.

§ 11 Schlussbestimmungen

Es gilt deutsches Recht. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Änderungen und Ergänzungen bedürfen der Textform. Im Übrigen gelten die Regelungen des Hauptvertrags.

Ort, Datum, Unterschrift Auftraggeber: _____

Ort, Datum, Unterschrift Auftragnehmer: _____

Anlage 1: Konkretisierung des Auftrags

[Projektbezeichnung, Umfang, Erhebungszeiträume, eingesetzte Instrumente – je Projekt zu konkretisieren.]

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DS-GVO)

1. Vertraulichkeit

- **Zutrittskontrolle:** Hosting ausschließlich in einem ISO-27001-zertifizierten Rechenzentrum der Hetzner Online GmbH in Deutschland; physischer Zutritt nur durch autorisiertes RZ-Personal.
- **Zugangskontrolle:** Serverzugriff ausschließlich über SSH-Public-Key-Verfahren (Ed25519), kein Passwort-Login; personalisierte Zugänge für einen eng begrenzten Administratorenkreis.
- **Zugriffskontrolle:** Datenbank ohne öffentliche Netzwerk-Exposition (nur internes Container-Netzwerk); rollenbasierte Datenbank-Berechtigungen; Container-Isolation (rootless).
- **Trennungskontrolle:** logische Trennung der Datenbestände nach Anwendungen und Projekten (getrennte Datenbankschemata); Studien- und Befragungsdaten getrennt von sonstigen Geschäftsdaten.
- **Pseudonymisierung:** Erhebungen werden, soweit methodisch möglich, pseudonymisiert oder anonym durchgeführt; Berichtslegung erfolgt aggregiert.

2. Integrität

- **Übertragungskontrolle:** Transportverschlüsselung sämtlicher Verbindungen per TLS; HTTP Strict Transport Security (HSTS) serverseitig erzwungen.
- **Eingabekontrolle:** Protokollierung administrativer Zugriffe und wesentlicher Verarbeitungsvorgänge; Zugriffs-Logs mit datenschutzkonformer IP-Maskierung.

3. Verfügbarkeit und Belastbarkeit

- Regelmäßige Datensicherungen auf ein getrenntes Speichermedium; dokumentiertes Wiederanlauf-Vorgehen.
- Aktuelle Systemsoftware (automatisch aktualisierendes Betriebssystem), Reverse-Proxy mit Sicherheits-Headern.

4. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung der Maßnahmen und der Serverkonfiguration; anlassbezogene Sicherheitsaudits; Datenschutz-Management durch den Inhaber.