Vertrag

zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

much. GmbH
Leopoldstraße 139
80804 München
Deutschland

–Auftragnehmer/Auftragsverarbeiter–

und

–Auftraggeber/Verantwortlicher–

Allgemeine Bestimmungen

1. Vertragsgegenstand

Dieser Vertrag zur Auftragsverarbeitung gemäß Art 28 DSGVO (nachfolgend **„Vertrag“**) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Gegenstand des Auftrags (Ziffer 4) in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte, personenbezogene Daten des Verantwortlichen verarbeiten.

2. Anwendung der EU Standardvertragsklauseln

Die Parteien legen diesem Vertrag die „Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR“ gemäß Durchführungsbeschluss der Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28(7) DS-GVO und Artikel 29(7) der Verordnung (EU) 2018/1725 vom 4. Juni 2021 (nachfolgend **„EU Standardvertragsklauseln“**) zugrunde. Auf die Standardklauseln kann über folgenden Link zugegriffen werden. https://muchconsulting.de/agb-de/

Die Anlagen 1-4 sind Bestandteil dieser Vereinbarung.

Dabei vereinbaren die Parteien folgende in den EU Standardvertragsklauseln aufgeführten Optionen:

- Klausel 1: Option 1
- Klausel 7.7: Option 2 mit Einspruchsfrist von 14 Tagen.
- Klausel 8.c.4: Option 1
- Klausel 9.1.b: Option 1
- Klausel 9.1.c: Option 1
- Klausel 9.2: Option 1

3. Abweichungen von den EU Standardvertragsklauseln

Die Parteien vereinbaren folgende Abweichungen von den EU Standardvertragsklauseln. Diese Abweichungen kommen im Falle von Widersprüchen gegenüber den EU Standardklauseln vorrangig zur Anwendung.

3.1. Einsatz von Unterauftragsverarbeitern (Klausel 7.7)

Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht fristgerecht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Servicevertrag und diesen Vertrag zum nächstmöglichen Zeitpunkt zu kündigen.

3.2. Unterstützung des Verantwortlichen (Klausel 8)

Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen. Bei der Unterstützung finden die Tagessätze des Hauptvertrags (AGB nach §2.3 Dienstleistungen) Anwendung.

3.3. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten (Klausel 9.1)

Sofern der Auftragnehmer für die Verletzung des Schutzes von Auftraggeber-Daten nicht verantwortlich ist, kann der Auftragnehmer vom Auftraggeber Ersatz für die in Ausübung der Unterstützungsleistungen nachgewiesenen enstandenen Aufwände und Kosten verlangen.

4. Gegenstand des Auftrags

Im Rahmen der Leistungserbringung nach dem Hauptvertrag ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten Dritter umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen sowie die sich aus der besonderen Stellung des Auftraggebers als Berufsgeheimnisträger ergebenden Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

5. Dauer des Auftrags

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags, sofern in diesem Vertrag nicht Abweichendes geregelt ist. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

6. Umfang, Art und Zweck der Datenverarbeitung

Die Tätigkeit des Auftragnehmers dient dem Zweck, dem Auftraggeber verschiedene Leistungen im Zusammenhang mit dem Hosting der ERP-Plattform odoo sowie Dienstleistungen hieran zu erbringen und wird vom Auftragnehmer in dem im Hauptvertrag vereinbarten Umfang erbracht. Der Inhalt des mitgeltenden Anlagenverzeichnisses spezifiziert dabei Anforderungen an die Tätigkeit des Auftragnehmers. Dabei erbringt der Auftragnehmer die folgenden Leistungen:

- ☐ Hosting einer odoo-Plattform
- ☐ Dienstleistungen an den odoo-Systemen des Auftraggebers

Ort: München

Datum: _____

Ort: _____

Datum: _____

_____

Auftragnehmer / Auftragsverarbeiter

Maximilian Rau, Geschäftsführer

Simon Stappen, Geschäftsführer

_____

Auftraggeber/Verantwortlicher

Anlagenverzeichnis:

Anlage 1	Datenarten / Kreise von Betroffenen
Anlage 2	Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO
Anlage 3	Weitere Auftragsverarbeiter
Anlage 4	Verantwortliche Stelle, Datenschutzbeauftragter und weisungsberechtigte Personen

Datenarten / Kreise von Betroffenen (Anlage 1)

1. Vom Auftrag umfasste Datenarten

Folgende Datenarten sind üblicherweise Gegenstand dieses Auftrags.

- ☑ Name
- ☑ Adressdaten
- ☑ Telefonnummer
- ☑ E-Mails
- ☑ Kommunikationsdaten
- ☑ Geräteinformation
- ☐ Standort
- ☐ Kaufhistorie
- ☐ Zahlungsdaten
- ☐ Gehalt
- ☐ alle weiteren ggf. auf der odoo-Plattform des Auftraggebers gespeicherten Daten sind ggf vom Auftraggeber zu vervollständigen:

2. Kreise von Betroffenen

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags:

- ☑ Beschäftigte des Auftraggebers
- ☑ Nutzer des Auftraggebers
- ☑ Kunden des Auftraggebers
- ☑ Interessenten des Auftraggebers
- ☑ Lieferanten und Dienstleister des Auftraggebers
- ☐ Auszubildende und Praktikanten des Auftraggebers
- ☐ Bewerber des Auftraggebers
- ☐ Betroffenenkreise sind ggf. vom Auftraggeber zu vervollständigen:

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO (Anlage 2)

Zum Zeitpunkt des Vertragsschlusses hat der Auftragnehmer folgende technisch organisatorischen Maßnahmen implementiert. Der Auftragnehmer ist aktuell ISO27001 und ISAE3402 SOC1 / SOC2 Zertifiziert.

Darüber hinaus werden alle Hosting Angebote in Rechenzentren der Hetzner Online GmbH betrieben. Ausführe Informationen zu Zutritts-, Zugangs-, Zugriffs-, Datenträger-, Trennungskontrolle, Integrität, Verfügbarkeit, Belastbarkeit finden Sie auch in den ToMs von Hetzner unter https://www.hetzner.com/AV/TOM.pdf.

I. Zweckbindung und Trennbarkeit
Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Logische Mandantentrennung (softwareseitig) in allen Softwaresystemen mit projektbasiertem Zugriffsmanagement
- Hosting Platform:
  - Trennung von Produktiv- und Testsystem auf unterschiedliche virtuelle Server
  - Logische Mandantentrennung durch virtuelle Server pro Kunde

II. Vertraulichkeit und Integrität
Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

1. Verschlüsselung
Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

- SSL bei Kommunikation über das Internet
- TLS 1.2+ / TLS 1.3 für alle Datenübertragungen (ältere Protokolle wie TLS 1.0/1.1, SSL, DES, 3DES, MD5, SHA-1 sind deaktiviert)
- AES-256 Verschlüsselung ruhender Daten (“at rest”)
- FileVault Full-Disk-Encryption auf allen Endgeräten
- SSH-Key-basierte Authentifizierung für Serverinfrastruktur
- Hosting-Plattform: SSL/TLS mit Let's Encrypt Zertifikaten

2. Pseudonymisierungs-Maßnahmen

- Der Auftraggeber ist für die Pseudonymisierung seiner Daten in den Anwendungen selbst verantwortlich.
- Für Testdatenbank ist einen Anonymisierung möglich mit dem kostenpflichtigen Anonymisierungsdienst

3. Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern (**Zutrittskontrolle**):

Hosting: Rechenzentrum bei Hetzner Online GmbH

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation Kunden für Colocation Racks
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters

Im Büro:

- Biometrisches oder mobile App mit biometrischen Freischaltung basiertes Schließsystem
- Aufzeichnung aller Zutritt mit digitaler Audit Trail für 90 Tage
- Videoüberwachung der Zugänge
- Keine Ausgabe von physischen Schlüsseln
- Sorgfältige Auswahl von Reinigungspersonal mit Kontrolle von polizeilichen Führungszeugnis beim Dienstleister

4. Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern **(Zugangskontrolle):**

- Zuordnung von Benutzerrechten, Zuordnung von Benutzerprofilen zu IT-Systemen
- Erstellen von Benutzerprofilen, Authentifikation mit Benutzername / Passwort, Passwortvergabe, Passwort-Richtlinien
- Nutzung von Passwort Managern, Single-Sign-On (“SSO”) und 2-Factor-Authentication (“2FA”)
- Zusätzliche Authentifizierung für alle Admins mit verpflichtenden FIDO-2 Schlüsseln
- RSA verschlüsselte SSH Keys bei Servern

- MDM verwaltet alle Endgeräte
- Endpoint Detection & Response (EDR) Lösung als Antivirus und Firewall auf allen Endgeräten
- Automatischen Sperrung von Endgeräten

5. Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**):

- Berechtigungskonzept Principle of Least Privilege
- Verwaltung der Rechte durch Systemadministrator
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
- Dokumentierten On- & Offboarding und Rollenwechsel Prozess
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Sofortige Sperrung aller Zugänge bei Ausscheiden (Remote-Lock/Wipe)
- Passwortmanager, Single-Sign-On (“SSO”) und 2-Factor-Authentication (“2FA”)
- Lokales Speichern von Unternehmens-/Kundendaten nur auf verwalteten und verschlüsselten Firmengeräten
- Hosting: Trennung von Kunden in eigenen virtuelle Server

6. Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**).

- Umfassende Logs in allen Systemen mit Kundendaten
- Hosting
    - Änderungen werden auf Serverseite geloggt
    - Änderungen werden in der Applikation nachverfolgt und sind für andere Nutzer sichtbar
    - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

7. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**).

- ISO 27001:2022 zertifiziertes ISMS (Zertifikat gültig bis 08.02.2029)
- Speicherung aller Daten und Zugänge mit projektbasierten Zugriff
- Jährliche Managementbewertung und interne Audits
- Weisungen werden in Textform erteilt, sofern nicht anders im Hauptvertrag geregelt. Sollte eine Weisung aufgrund ihrer Dringlichkeit mündlich erteilt worden sein, wird der Auftraggeber sie unverzüglich schriftlich (oder: in Textform) nachsenden.
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnnis und Datenschutzschulungen
- Externer DSB (aktuell: Dr. Jochen Notholt) und jährliches DPO-Audit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags gemäß Hauptvertrag

8. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (**Transport- bzw. Weitergabekontrolle**):

- Ausschließliche Nutzung verschlüsselter Kanäle (HTTPS, verschlüsselte APIs)
- Credentials ausschließlich über 1Password Vaults oder über 2 End-2-End verschlüsselte Kanäle
- Keine Nutzung von USB-Sticks oder externen Datenträgern gestattet
- Transport und Weitergabe an Dritte nur aufgrund von einschlägigen Rechtsgrundlage und unter Anwendung angemessener Sicherheitsmaßnahmen wie
    - Einsatz von verschlüsselten “SSH-Tunneln”
    - Einsatz von verschlüsselte Übertragung (“SSL”)
    - Verschlüsselung physischer Datenträger

  weitergeben

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

- Hosting
    - Regelmäßige Updates der Software

- Täglich Backups mit Speicherung auf mindestens 2 redundanten Backup-Systemen. Es werden zu jedem Zeitpunkt mindestens fünf Backups aufbewahrt. Der Kunde trägt die Verantwortung, eigene Kopien der Backups anzufertigen.
- Regelmäßige Tests der Wiederherstellungsverfahren

IV. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen
Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen nach Ermessen oder anlassbezogen prüfen, evaluieren und bei Bedarf anpassen. Der in den TOM angegebene Sicherheitsstandard wird auch bei einer Anpassung der Maßnahmen zu keinem Zeitpunkt unterschritten.

Zusätzlich erfolgen fortlaufenden Management IT Security Reviews und ein jährliches externes ISO 27001 Audit.

Weitere Auftragsverarbeiter (Unterauftragnehmer) (Anlage 3)

Name und Anschrift der Unterauftragnehmer / weiteren Auftragsverarbeiter	**Gegenstand der Unterbeauftragung**	**Sitz des Auftragsverarbeiters**
Hetzner Online GmbH Industriestr 25 91710 Gunzenhausen	Hosting und Bereitstellung von Rechenzentrumsleistungen	Deutschland
much. Consulting - Unipessoal LDA, Av 5 de Outubro 146, 1050-061 Lisboa, Portugal (Tochter der much. GmbH)	Erbringen von Dienstleistungen gemäß Hauptvertrag	Portugal
Zukunft digitale und offene Verwaltung GmbH, Leopoldstraße 31,80802 München (Tochter der much. GmbH)	Erbringen von Dienstleistungen gemäß Hauptvertrag	Deutschland
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland	Bereitstellung von Cloud-basierten Produktivitäts- und Kollaborationsdiensten (Google Workspace) mit Datenspeicherung innerhalb der EU, einschließlich E-Mail, Dateispeicherung, Kalender und Videokonferenzen, im Rahmen der Dienstleistungen gemäß Hauptvertrag	Ireland

Verantwortliche Stelle, Datenschutzbeauftragter und weisungsberechtigte Personen (Anlage 4)

Benennung der verantwortlichen Stelle zur Meldung nach Art. 12 bis 22 oder Art. 33 DSGVO
Im Falle eines Verstoßes gegen die genannten Artikel der DSGVO erfolgt die Meldung immer zuerst an die folgende Stelle:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18,
91504 Ansbach
Telefon: +49 (0) 981 180093-0
Telefax: +49(0) 981 180093-800
E-Mail: poststelle@lda.bayern.de

Nennung des ernannten Datenschutzbeauftragen des Auftragsverarbeiters
Der Auftragsverarbeiter hat folgende Person als Datenschutzbeauftragten bestellt:

Dr. Jochen Notholt Rechtsanwalt & DSB (TÜV)
Lindwurmstraße 10
80337 München
E-Mail: jn@comp-lex.de

Benennung weisungsberechtigter Personen
Die Benennung der weisungsberechtigten Personen erfolgt fortlaufend im Projekt zwischen den Parteien in Textform. Falls nicht anders geregelt, sind alle Geschäftsführer, Prokuristen und zusätzlich hier aufgelisteten Führungskräfte des Auftragsverarbeiters weisungsberechtigt:

Simon Stappen, Geschäftsführer, simon.stappen@muchconsulting.de
Maximilian Rau, Geschäftsführer, maximilian.rau@muchconsulting.de
Samuel Reinhardt, Prokurist, samuel.reinhardt@muchconsulting.de

In Notfällen auch an emergencies@muchconsulting.de wenden.