# Vertrag

# zur Auftragsverarbeitung

# gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

**Zukunft digitale und offene Verwaltung GmbH**
**Leopoldstraße 31**
**80802 München**

und

–Auftragnehmer/Auftragsverarbeiter–

–Auftraggeber/Verantwortlicher–

## Abschnitt 1 – 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://zdov.de/agb/

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

Klauseln 2 und 4 der EU Standardvertragsklauseln finden keine Anwendung.

### 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 30 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. Hierbei finden die Konditionen des Hauptvertrags 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 entstehenden nachzuweisenden 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 | Ort: _____ |
| Datum: _____ | Datum: _____ |
| _____ | _____ |
| Auftragnehmer / Auftragsverarbeiter | 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 und weisungsberechtigte Personen

**Datenarten / Kreise von Betroffenen (Anlage 1)**

## 1. Vom Auftrag umfasste Datenarten

Folgende Datenarten sind üblicherweise Gegenstand dieses Auftrags.

☒ Name

☒ Adressdaten

☒ Standort

☒ Zahlungsdaten

☒ Kaufhistorie

☒ Geräteinformation

☒ Gehalt

☒ Kommunikationsdaten

☒ E-Mails

☒ Telefonnummer

☒ 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

☒ Auszubildende und Praktikanten des Auftraggebers

☒ Bewerber des Auftraggebers

☒ Nutzer des Auftraggebers

☒ Kunden des Auftraggebers

☒ Interessenten des Auftraggebers

☒ Lieferanten und Dienstleister des Auftraggebers

☒ Interessenten

☒ Lieferanten und Dienstleister

☒ 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.**

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 der Software und durch virtuelle Server pro Kunde Berechtigungskonzept
- Trennung von Produktiv- und Testsystem auf unterschiedliche virtuelle Server

**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: Einsatz von Secure Sockets Layer bei der Kommunikation über das Internet, solange dies vom Auftraggeber unterstützt wird.

2. Pseudonymisierung
„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

- Nein. Der Auftraggeber ist für die Pseudonymisierung seiner Daten in den Anwendungen selber zuständig.

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

**Im 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:**

- Chipkarten-/Transponder-Schließsystem
- Videoüberwachung der Zugänge
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal

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
- RSA verschlüsselte SSH Keys bei Servern
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall

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**):

- Trennung von Kunden in eigenen virtuelle Server
- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. Bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge

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**).

- 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**).

- Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

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**):

- Einsatz von SSH-Tunneln
- Verschlüsselung physischer Datenträger

**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

- Regelmäßige Updates der Betriebssysteme und von unserer bereitgestellten Software
- Täglich Backups mit Speicherung auf dem Server des Kunden und 2 weiteren Backup Systemen. Es werden zu jedem Zeitpunkt mindestens fünf Backups aufbewahrt. Der Kunde trägt die Verantwortung eigene Kopien der Backups anzufertigen.
- Odoo Backups werden vollständig und installierbar bereitgestellt

**IV. Besondere Datenschutzmaßnahmen**

Es wurden keine besonderen Datenschutzmaßnahmen ergriffen.

**V. 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.

**Weitere Auftragsverarbeiter (Unterauftragnehmer) (Anlage 3)**

| **Name und Anschrift der Unterauftragnehmer / weiteren Auftragsverarbeiter** | **Gegenstand der Unterbeauftragung** | **Sitz des Auftragsverarbeiters** |
|---|---|---|
| much. GmbH<br>Marcel-Breuer-Straße 17<br>80807 München<br>(Muttergesellschaft der ZdoV) | Erbringen von Dienstleistungen gemäß Hauptvertrag | Deutschland |
| Manvetipon - Unipessoal LDA,<br>Av. Fontes Pereira de Melo 3,<br>1050-005 Lisboa, Portugal<br>(Tochter der much. GmbH) | Erbringen von Dienstleistungen gemäß Hauptvertrag | Portugal |
| Hetzner Online GmbH<br>Industriestr 25<br>D-91710 Gunzenhausen | Hosting und Bereitstellung von Rechenzentrumsleistungen (nur bei Hosting durch ZdoV) | Deutschland |
| | | |
| | | |
| | | |

**Verantwortliche Stelle 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

**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:

Finnigan Lutz, Geschäftsführer, finnigan.lutz@zdov.de
Nicolas Colsman, Geschäftsführer, nicolas.colsman@zdov.de