

# Auftragsverarbeitungsvertrag (AVV)

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag gemäss Artikel 28 der Datenschutz-Grundverordnung (DSGVO)

## Vertragsparteien

Dieser Auftragsverarbeitungsvertrag (nachfolgend „Vertrag“ oder „AVV“) wird geschlossen zwischen:

**Merkas Technologies GmbH**, vertreten durch den Geschäftsführer Nikola Merkas, Brauerstrasse 27, 8004 Zürich, Schweiz (nachfolgend „Auftragnehmer“)

— und —

dem **Kunden der OKR App**, der sich registriert und einen kostenpflichtigen oder kostenlosen Workspace nutzt (nachfolgend „Auftraggeber“ oder „Verantwortlicher“).

Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, der Auftragnehmer ist Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Rahmen der Nutzung der OKR App.

Dieser AVV wird durch Bestätigung im Rahmen der Workspace-Erstellung bzw. der Registrierung wirksam und ist Bestandteil der Allgemeinen Geschäftsbedingungen des Auftragnehmers.

## 1. Gegenstand und Dauer der Verarbeitung

### 1.1 Gegenstand

Gegenstand des Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Bereitstellung der OKR App, einer webgestützten Software-as-a-Service-Plattform zur Verwaltung von Objectives and Key Results (OKRs).

### 1.2 Dauer

Die Dauer dieses Vertrags entspricht der Laufzeit des zugrundeliegenden Nutzungsverhältnisses (Hauptvertrag). Der Vertrag endet automatisch mit Beendigung des Nutzungsverhältnisses, unbeschadet der Pflichten zur Löschung oder Rückgabe der Daten nach Ziffer 9.

## 2. Art, Umfang und Zweck der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich zum Zweck der Bereitstellung und des Betriebs der OKR App. Die Verarbeitung umfasst insbesondere das Erheben, Erfassen, Speichern, Anpassen, Auslesen, Verwenden, Löschen und Vernichten von Daten im Rahmen der vertraglich vereinbarten Leistungen.

Folgende Tätigkeiten werden im Auftrag erbracht:

- Bereitstellung der OKR-Management-Funktionen (Objectives und Key Results)
- Verwaltung von Workspaces, Nutzern, Einladungen und Mitgliedschaften
- Authentifizierung und Zugriffskontrolle
- Speicherung und Hosting der Kundendaten auf Servern in der EU
- Bereitstellung von Dashboards und Fortschrittsanzeigen
- Technischer Support und Fehlerbehebung

## 3. Kategorien betroffener Personen und Daten

### 3.1 Kategorien betroffener Personen

- Mitarbeitende und Führungskräfte des Auftraggebers
- Vom Auftraggeber eingeladene Nutzer (z.B. externe Partner oder Berater)

### 3.2 Kategorien personenbezogener Daten

- Stammdaten: Name, E-Mail-Adresse, Profilangaben
- Zugangsdaten: Passwort-Hashes, Authentifizierungsdaten
- Nutzungsdaten: Login-Zeitpunkte, Aktivitäten, Workspace-Zugehörigkeit
- Inhaltsdaten: Objectives, Key Results und zugehörige Angaben (z.B. Beschreibungen, Werte), soweit diese personenbezogene Daten enthalten
- Kommunikationsdaten: Support-Anfragen, Feedback

**Hinweis:** Die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO ist nicht Gegenstand dieses Vertrags. Der Auftraggeber verpflichtet sich, keine solchen Daten in die OKR App einzugeben.

## 4. Weisungsrecht des Auftraggebers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO).

Die Nutzung der OKR App durch den Auftraggeber gemäss der bereitgestellten Funktionen gilt als Erteilung der entsprechenden Weisungen. Darüber hinausgehende Einzelweisungen sind in Textform (z.B. per E-Mail) zu erteilen.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen geltendes Datenschutzrecht verstösst.

## 5. Technische und organisatorische Massnahmen (TOM)

Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Hierzu zählen insbesondere:

- **Verschlüsselung:** Verschlüsselte Datenübertragung per TLS 1.2 oder höher
- **Pseudonymisierung:** Passwörter werden ausschliesslich als kryptografische Hashes gespeichert
- **Zugriffskontrolle:** Trennung der Daten je Workspace und Verwaltung des Zugangs über Administratorrechte innerhalb der Anwendung sowie Zugriffskontrollen auf Infrastrukturebene
- **Verfügbarkeit:** Regelmässige automatisierte Backups
- **Belastbarkeit:** Massnahmen zur Wiederherstellung der Verfügbarkeit nach einem physischen oder technischen Zwischenfall
- **Vorfälle:** Im Fall eines Sicherheitsvorfalls erfolgt eine umgehende Reaktion sowie die Erfüllung der gesetzlichen Melde- und Benachrichtigungspflichten (Art. 33 und 34 DSGVO)

Die Massnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer ist berechtigt, alternative angemessene Massnahmen umzusetzen, sofern das Schutzniveau nicht unterschritten wird.

## 6. Unterauftragsverarbeiter

Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Der Auftragnehmer setzt zum Zeitpunkt des Vertragsschlusses folgende Unterauftragsverarbeiter ein:

| Anbieter                     | Zweck                            | Standort         |
|------------------------------|----------------------------------|------------------|
| Strato AG                    | Hosting und Server-Infrastruktur | EU (Deutschland) |
| Stripe Payments Europe, Ltd. | Zahlungsabwicklung               | EU (Irland)      |

Der Auftragnehmer stellt sicher, dass mit jedem Unterauftragsverarbeiter vertragliche Verpflichtungen bestehen, die den Anforderungen dieses Vertrags und Art. 28 DSGVO entsprechen.

Beabsichtigt der Auftragnehmer, einen Unterauftragsverarbeiter hinzuzufügen oder zu ersetzen, informiert er den Auftraggeber rechtzeitig in Textform oder durch Aktualisierung der veröffentlichten Liste. Der Auftraggeber kann der Änderung innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Im Falle eines berechtigten Widerspruchs ist der Auftragnehmer berechtigt, das Nutzungsverhältnis zu beenden.

## 7. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich insbesondere:

- die Daten ausschliesslich im Rahmen der Weisungen des Auftraggebers zu verarbeiten
- die zur Verarbeitung befugten Personen zur Vertraulichkeit zu verpflichten (Art. 28 Abs. 3 lit. b DSGVO)
- die technischen und organisatorischen Massnahmen nach Art. 32 DSGVO einzuhalten
- den Auftraggeber bei der Erfüllung der Betroffenenrechte (Art. 12-23 DSGVO) zu unterstützen
- den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32-36 DSGVO zu unterstützen (Datensicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung)
- dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mitzuteilen
- nach Wahl des Auftraggebers alle Daten nach Abschluss zu löschen oder zurückzugeben
- dem Auftraggeber die zum Nachweis der Einhaltung erforderlichen Informationen bereitzustellen

## 8. Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmässigkeit der Datenverarbeitung verantwortlich. Er verpflichtet sich insbesondere:

- nur Daten in die OKR App einzugeben, für deren Verarbeitung eine Rechtsgrundlage besteht
- die betroffenen Personen, soweit erforderlich, über die Datenverarbeitung zu informieren
- keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO einzugeben
- Zugangsdaten vertraulich zu behandeln und Berechtigungen sorgfältig zu vergeben

## 9. Löschung und Rückgabe von Daten

Nach Beendigung des Nutzungsverhältnisses oder auf Weisung des Auftraggebers löscht der Auftragnehmer die personenbezogenen Daten des Auftraggebers, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

Auf Anfrage stellt der Auftragnehmer dem Auftraggeber dessen Daten vor der Löschung in einem gängigen, maschinenlesbaren Format zur Verfügung. Backups werden im Rahmen der regulären Backup-Zyklen automatisch überschrieben.

## 10. Nachweise und Kontrollen

Der Auftragnehmer weist dem Auftraggeber auf Anfrage die Einhaltung der in diesem Vertrag festgelegten Pflichten in geeigneter Weise nach, beispielsweise durch Bereitstellung einer aktuellen Dokumentation der technischen und organisatorischen Massnahmen.

Kontrollen vor Ort werden auf das erforderliche Mass beschränkt, rechtzeitig angekündigt und so durchgeführt, dass der Geschäftsbetrieb des Auftragnehmers nicht unverhältnismässig beeinträchtigt wird.

## 11. Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO sowie den Regelungen des zugrundeliegenden Hauptvertrags (Allgemeine Geschäftsbedingungen). Im Verhältnis der Parteien untereinander gelten die dort vereinbarten Haftungsbeschränkungen, soweit gesetzlich zulässig.

## 12. Schlussbestimmungen

Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Anstelle der unwirksamen Bestimmung gilt eine Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV in Bezug auf den Datenschutz vor. Es gilt das Recht der Bundesrepublik Deutschland.

**Annahme:** Dieser Auftragsverarbeitungsvertrag wird durch elektronische Bestätigung im Rahmen der Workspace-Erstellung bzw. Registrierung rechtswirksam geschlossen. Auf Wunsch von Geschäftskunden kann eine individuell unterzeichnete Fassung bereitgestellt werden.

---

Ort, Datum

---

Ort, Datum

---

Auftragnehmer (Merkas Technologies GmbH)

---

Auftraggeber (Kunde)