Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen dem mein_werkzeugkoffer Kunden (Verantwortlicher) und der Inventory ONE GmbH (Auftragsverarbeiter), Steinbeisstr. 12, 73037 Göppingen wird nachfolgender Vertrag geschlossen.

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Vertrag über die Nutzung der in Ziffer 1 näher bezeichneten Software mein_werkzeugkoffer (im Weiteren Lizenzvereinbarung) des Auftragsverarbeiters durch den Verantwortlichen. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Umsetzung eigener Geschäftszwecke im Zusammenhang mit dem Dienstleistungsvertrag – eine Übertragung von ‚Funktionen' ist ausdrücklich nicht beabsichtigt.

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

In dem im Bestellprozess erworbenen mein_werkzeugkoffer gehören dazu im Kern (1) die Inventarverwaltung, (2) die Zuweisung des Inventars auf Empfänger und (3) die Dokumentation der Historie des Inventars.

In dem im Bestellprozess erworbenen mein_werkzeugkoffer ist es zudem möglich, Dokumente und Bilder zu Inventar hochzuladen. Dieses kann innerhalb von mein_werkzeugkoffer von Benutzern, je nach Berechtigung, eingesehen werden. Dabei trägt der Verantwortliche die volle Verantwortung für die hochgeladenen Dateien, deren Inhalt vom Auftragsverarbeiter nicht geprüft wird.

Der Gegenstand dieses Auftrags ergibt sich im Übrigen aus der bestehenden Lizenzvereinbarung, auf die hier verwiesen wird (im Weiteren „Lizenzvereinbarung"). Dabei handelt es sich um die Verarbeitung personenbezogener Daten (im Weiteren „Daten") durch den Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit der Nutzung von mein_werkzeugkoffer.

1.2 Dauer der Vereinbarung

Die Laufzeit dieses Vertrages entspricht der Laufzeit der Lizenzvereinbarung.

2. Konkretisierung des Auftragsverhältnisses

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragsverarbeiter erhält Zugriff auf die bei der Benutzung der in der vertragsgegenständlichen Software gespeicherten personenbezogenen Daten und nutzt diese zum Zweck der Leistungserbringung. Der Umfang der vorgenommenen Erhebung, Verarbeitung und Nutzung dieser Daten richtet sich dabei nach den Leistungen und dem Funktionsumfang des Produktes.

Folgende Datenkategorien können vom Verantwortlichen durch direkte Eingabe oder durch Hochladen in mein_werkzeugkoffer verarbeitet werden:

Angabe zu Mitbenutzern (Empfänger) in mein_werkzeugkoffer. Name, Vorname, E-Mail-Adresse, Handynummer, Personalnummer, Abteilung, Zeitstempel des letzten Logins, durchgeführte Aktionen innerhalb von mein_werkzeugkoffer

Alle Kernfunktionen von mein_werkzeugkoffer werden ausschließlich in Deutschland entwickelt und. Darüber hinaus gibt es ergänzende Zusatzfunktionen, bei der auf durch den Verantwortlichen genehmigte Subunternehmen (siehe Anlage 1) zurückgegriffen wird, die teilweise ihren Sitz außerhalb der EU/EWR haben.

Jede weitere Verlagerung einer Datenverarbeitung in ein Drittland außerhalb der EU/EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in den USA wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO).

2.2 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitbenutzer (Empfänger), die durch den Verantwortlichen zur Mitarbeit in mein_werkzeugkoffer freigeschaltet werden, z.B. Administratoren, Verantwortliche der Inventarverwaltung, Mitarbeiter denen Inventar zugewiesen wird

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragsverarbeiter verpflichtet externe Rechenzentren sowie sonstige Unterauftragsverarbeiter, die innerbetriebliche Organisation so zu gestalten, dass es den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere findet die Datenverarbeitung auf Datenverarbeitungsanlagen statt, für die das Rechenzentrum oder der sonstige Unterauftragsverarbeiter alle technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

3.2 Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten in Anlage 2).

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

4.2 Der Auftragsverarbeiter wird die Daten des Verantwortlichen nach dem Ende der Lizenzvereinbarung wie folgt behandeln:

a. Der Account bleibt im kostenlosen Deaktiviert-Modus. Spätestens 12 Monate nach Ende der Lizenzvereinbarung werden die Daten gelöscht.
b. Der Verantwortliche kann jederzeit vollständige Löschung verlangen.

c. Der Verantwortliche kann jederzeit die Inventar Daten exportieren.
d. Entschließt sich ein Verantwortlicher nach der kostenlosen Testphase nicht zum Kauf eines mein_werkzeugkoffer Abonnements, so wird der Testaccount nach einem letztmaligen Hinweis per E-Mail automatisch spätestens 12 Monate nach Beendigung der Testregistrierung gelöscht.

Darüber hinaus sind zusätzliche Löschkonzepte, das Recht auf Vergessenwerden, die Berichtigung und Auskunft vom Verantwortlichen sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit (inklusive § 203 StGB) verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
b. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in Anlage 2).
c. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
d. Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
e. Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der

Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

f. Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
g. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

a. Als Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice erbringt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
b. Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel der bestehenden genehmigten Unterauftragsverarbeiter sind zulässig, soweit der Auftragsverarbeiter eine solchen Einschaltung von Unterauftragsverarbeitern dem Verantwortliche eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird. Im Falle des Einspruchs des Verantwortlichen steht dem Auftragsverarbeiter ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung zu.
c. Der Verantwortliche stimmt der Beauftragung der in der Anlage 1 vor Beginn der Verarbeitung mitgeteilten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

d. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.
e. Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7. Kontrollrechte des Verantwortlichen

a. Der Verantwortliche hat nach Vorankündigung das Recht, die Einhaltung der über die datenschutzrechtlichen Prozesse und der vertraglichen Vereinbarung durch den Auftragsverarbeiter oder das externe Rechenzentrum/den Unterauftragsverarbeiter zu kontrollieren. Dies kann durch die Einholung von Auskünften erfolgen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.
b. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8. Mitteilung bei Verstößen des Auftragsverarbeiters

a. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
    - die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte

Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
    - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
    - die Verpflichtung, den Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
    - die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung
    - die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
b. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

9.Weisungsbefugnis des Verantwortlichen

a. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).
b. Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

a. Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

b. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Für die Löschung der Daten in der Applikation gilt Nr. 4.
c. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

11. Schlussbestimmungen

Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO tritt mit Unterzeichnung in Kraft und ersetzt alle zuvor geschlossenen Vereinbarungen zur Auftragsverarbeitung.

Anlage 1: Unterauftragsverarbeiter

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Nr.	Firma	Anschrift	Leistung
1	Google	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043,USA	Google Firebase: • Cloud Functions Starten von Backup-Prozessen • Cloud Storage Speichern von hochgeladenen Dokumenten Google Firestore: Nach Mandanten getrennte Speicherung der Anwendungsdaten

Anlage 2: Technische und organisatorische Maßnahmen

der Inventory ONE GmbH

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle:

- Büroräume allgemein:
  Der Zugang zum Gebäude und den Büroräumen ist durch verschlossene Türen beschränkt. Mitarbeiter:innen haben nur Schlüssel für Räume, die zur vertraglich vereinbarten Arbeit notwendig sind. Der Zugang in Räume in denen sensible Informationen gelagert werden, ist auf die Geschäftsführung beschränkt.
- Rechenzentrumsräume:
  Kundendaten werden in Rechenzentren von Hetzner in Frankfurt verarbeitet und Google Firestore in Frankfurt gespeichert.

1.2. Zugangskontrolle:

- Der Benutzer- und Administratorzugriff auf das mein_werkzeugkoffer System beruht auf einem rollenbasierten Zugriffsberechtigungsmodell. Damit wird sichergestellt, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Es existieren Regeln zur Passwortkomplexität.
- Es gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.
- Der Zugriff auf Serversysteme erfolgt SSH-verschlüsselt („Public key“).

1.3. Zugriffskontrolle:
- Zugriffsberechtigung auf mein_werkzeugkoffer Produktivsysteme ist auf dich Geschäftsführung beschränkt

1.4. Trennungskontrolle:
- Datensätze unterschiedlicher mein_werkzeugkoffer Kunden werden in einer einheitlichen Datenbank getrennt in kundenspezifische Bereiche gespeichert. Der Zugriff auf Kundendaten aus anderen Kundenbereichen in der Datenbank ist durch Sicherheitsregeln ausgeschlossen.
- Test- und Produktivdaten sind strikt getrennt in unabhängigen Systemen, Entwicklungssysteme sind ebenfalls unabhängig von Test- und Produktivsystemen
- Unterschiedliche Domains und SSL-Zertifikate für Test- und Produktivsysteme

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle:
- Datenübertragung zwischen mein_werkzeugkoffer Serversystemen erfolgt ausschließlich innerhalb abgegrenzter und durch Bastion-Hosts abgeschirmter Subsysteme
- Soweit Daten zu beauftragten Partnern übertragen werden, sind diese Datenübertragungskanäle immer TLS verschlüsselt
- Datenabrufe und Übermittlungsaktivitäten werden protokollier

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle:
- Es werden regelmäßig automatische Sicherungskopien und Backups aller mein_werkzeugkoffer Kundendaten erstellt

- Es gibt ein dediziertes Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können (Datenintegrität der Backups)
- Backups und Sicherungskopien sind über mehrere redundante Serversysteme

3.2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):

- Redundante Auslegung von Serversystemen und Datenbanken
- Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft

Stand: 30.09.2024