Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

dem Auftraggeber — dem Nutzer (im Folgenden „Auftraggeber" oder „Kunde"), der mit dem Anbieter einen Hauptvertrag über die Nutzung der Software „Craftity" (im Folgenden „Hauptvertrag") abgeschlossen hat —

und

dem Auftragnehmer

Daniel Mandsfeld – Craftity
Einzelunternehmen
Brufertstr. 10
76437 Rastatt
Deutschland
USt-IdNr.: DE 462 397 050
E-Mail: hallo@craftity.de
Web: craftity.de

(im Folgenden „Auftragnehmer" oder „Anbieter").

Präambel

Der Anbieter stellt dem Kunden eine cloudbasierte Software-as-a-Service-Lösung („Craftity") zur Verfügung, mit der der Kunde Kundendaten, Projekte, Angebote, Rechnungen, Zeiterfassungen, Mitarbeiterdaten und projektbezogene Fotos verwalten kann. Im Rahmen dieser Nutzung verarbeitet der Anbieter im Auftrag des Kunden personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO. Die Parteien schließen daher diesen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.

Dieser AVV gilt mit Abschluss des Hauptvertrags als geschlossen und hat während dessen gesamter Laufzeit Gültigkeit. Bei Widersprüchen zwischen diesem AVV und den AGB des Hauptvertrags hat dieser AVV Vorrang.

---

§ 1 Gegenstand und Dauer

1. Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Bereitstellung der Software „Craftity" gemäß Hauptvertrag.

2. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Nach Beendigung des Hauptvertrags gelten die Regelungen aus § 10 dieses Vertrags zur Löschung bzw. Rückgabe der Daten.
3. Der Auftragnehmer ist berechtigt, in begründeten Fällen (z. B. bei gesetzlichen Änderungen, neuen aufsichtsbehördlichen Vorgaben oder Aufnahme neuer Sub-Auftragsverarbeiter) Anpassungen dieses AVV vorzunehmen. Der Auftraggeber wird über solche Änderungen mit angemessener Frist von mindestens vier Wochen in Textform informiert.

---

§ 2 Art und Zweck der Verarbeitung

1. Die Verarbeitung erfolgt ausschließlich zum Zweck der Bereitstellung und des Betriebs der Software „Craftity" sowie zur Erbringung der im Hauptvertrag beschriebenen Leistungen.
2. Die Verarbeitung umfasst insbesondere folgende Tätigkeiten:

- Speichern, Anzeigen, Verändern, Übermitteln und Löschen von Stamm- und Bewegungsdaten innerhalb der Anwendung
- Generierung und Versand von Dokumenten (Angeboten, Rechnungen, Lieferscheinen) an vom Auftraggeber bestimmte Empfänger
- Speicherung von projektbezogenen Foto-Uploads
- Erstellung und Verwaltung von Backups
- Bereitstellung von Export- und Auswertungsfunktionen für den Auftraggeber

3. Die Verarbeitung der Daten erfolgt regelmäßig innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Soweit einzelne Sub-Auftragsverarbeiter ihren Unternehmenssitz außerhalb der EU/EWR haben (siehe Anlage 2), erfolgt die tatsächliche Verarbeitung gleichwohl in EU-Rechenzentren; eine Drittlandübermittlung im Sinne der Art. 44 ff. DSGVO ist in diesen Fällen jedoch nicht vollständig auszuschließen. Sie wird auf Grundlage der EU-Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914 abgesichert.

---

§ 3 Art der Daten und Kreis der Betroffenen

1. **Datenkategorien**, die im Auftrag des Auftraggebers verarbeitet werden:

- Stammdaten (Name, Anschrift, Kunden-/Lieferantennummer)
- Kontaktdaten (Telefon, E-Mail)
- Vertrags- und Auftragsdaten (Angebote, Aufträge, Rechnungen, Zahlungen)
- Kommunikationsdaten (z. B. Notizen und Tagebucheinträge)
- Arbeitszeit- und Abwesenheitsdaten von Mitarbeitenden
- Foto- und Bilddaten, ggf. mit abgebildeten Personen

- Bei Mitarbeitenden: ggf. Stundenlohn, Vertragsdaten

2. **Kreis der Betroffenen**:

- Endkunden des Auftraggebers (natürliche Personen oder Ansprechpartner bei juristischen Personen)
- Lieferanten und Geschäftspartner des Auftraggebers
- Mitarbeitende und freie Mitarbeiter des Auftraggebers
- Sonstige Personen, die ggf. auf Baustellen-Fotos abgebildet sind

3. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden im Regelbetrieb nicht verarbeitet. Der Auftraggeber stellt sicher, dass derartige Daten nicht oder nur in zulässigem Umfang in die Software eingegeben werden.

---

§ 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisungen des Auftraggebers. Der Hauptvertrag und dieser AVV gelten als solche Weisungen. Zusätzliche Einzelweisungen sind in Textform zu erteilen.
2. Sieht sich der Auftragnehmer aufgrund einer rechtlichen Verpflichtung (z. B. nach EU- oder mitgliedstaatlichem Recht) zur Verarbeitung gezwungen, die einer Weisung widerspricht, teilt er dies dem Auftraggeber vor der Verarbeitung mit, sofern das Recht eine solche Mitteilung nicht ausdrücklich verbietet.
3. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt.
4. Der Auftragnehmer setzt die in Anlage 1 dieses Vertrags beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO um und hält diese während der Vertragslaufzeit auf dem aktuellen Stand der Technik.
5. Der Auftragnehmer verpflichtet alle Personen, die zur Verarbeitung der personenbezogenen Daten befugt sind, zur Vertraulichkeit, soweit sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.
6. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Beantwortung von Anfragen betroffener Personen (Art. 12 ff. DSGVO) sowie bei der Erfüllung der Pflichten aus Art. 32 bis 36 DSGVO.
7. Der Auftragnehmer hat keinen geschäftsführenden Datenschutzbeauftragten nach Art. 37 DSGVO bestellt, da die Voraussetzungen nicht vorliegen. Anfragen mit Datenschutzbezug sind an `hallo@craftity.de` zu richten.

---

§ 5 Pflichten des Auftraggebers

1. Der Auftraggeber ist im Rahmen dieses Vertrags „Verantwortlicher" im Sinne von Art. 4 Nr. 7 DSGVO. Er ist allein verantwortlich für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen.
2. Der Auftraggeber stellt sicher, dass für die in die Software eingegebenen personenbezogenen Daten eine ausreichende Rechtsgrundlage (Art. 6 DSGVO, ggf. Art. 9 DSGVO) besteht.
3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er bei der Auftragsdurchführung Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen feststellt.
4. Der Auftraggeber benennt einen Ansprechpartner für datenschutzrechtliche Belange. Sofern kein eigener Datenschutzbeauftragter bestellt ist, fungiert der gesetzliche Vertreter des Auftraggebers als Ansprechpartner.

---

§ 6 Sub-Auftragsverarbeiter

1. Der Auftraggeber erteilt dem Auftragnehmer mit Abschluss dieses Vertrags die allgemeine Genehmigung zur Hinzuziehung von Sub-Auftragsverarbeitern. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Sub-Auftragsverarbeiter sind in **Anlage 2** dieses Vertrags abschließend aufgeführt.
2. Der Auftragnehmer schließt mit jedem Sub-Auftragsverarbeiter einen Vertrag, der diesem mindestens die gleichen Datenschutzpflichten auferlegt wie der vorliegende AVV dem Auftragnehmer.
3. Bei Hinzuziehung eines weiteren oder Austausch eines bestehenden Sub-Auftragsverarbeiters informiert der Auftragnehmer den Auftraggeber spätestens vier Wochen vor der geplanten Änderung in Textform. Der Auftraggeber kann gegen die Änderung innerhalb dieser Frist aus berechtigtem Grund unter Hinweis auf konkrete datenschutzrechtliche Bedenken Widerspruch einlegen. Im Falle eines berechtigten Widerspruchs ist der Auftraggeber berechtigt, den Hauptvertrag außerordentlich zu kündigen.
4. Nicht als Sub-Auftragsverarbeiter im Sinne dieses Vertrags gelten Dienstleister, die als eigenständig Verantwortliche tätig werden, insbesondere Zahlungsdienstleister (z. B. die Mollie B.V. für die Abwicklung der monatlichen Vergütung). Auf deren Datenverarbeitung findet dieser AVV keine Anwendung.

---

§ 7 Technische und organisatorische Maßnahmen (TOMs)

1. Der Auftragnehmer trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus nach Art. 32 DSGVO.
2. Die Maßnahmen können während der Vertragslaufzeit an den jeweiligen Stand der Technik angepasst werden. Wesentliche Verschlechterungen des Schutzniveaus sind unzulässig.
3. Detaillierte Beschreibungen der technischen Umsetzung können auf Anfrage in Textform vom Auftragnehmer übermittelt werden, sofern dem keine überwiegenden Sicherheitsinteressen entgegenstehen.

---

§ 8 Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, sich vor Beginn der Datenverarbeitung sowie regelmäßig während der Vertragslaufzeit von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
2. Der Nachweis erfolgt vorrangig durch:

- Bereitstellung eines aktuellen Berichts über die getroffenen TOMs,
- Vorlage geeigneter Zertifizierungen oder Testate (z. B. ISO 27001 der eingesetzten Sub-Auftragsverarbeiter),
- Beantwortung eines vom Auftraggeber übermittelten Fragenkatalogs in Textform.

3. Sofern in Einzelfällen eine Vor-Ort-Prüfung erforderlich ist, wird diese mit angemessener Ankündigungsfrist (mindestens vier Wochen), während üblicher Geschäftszeiten und ohne Störung des Betriebsablaufs durchgeführt. Vor-Ort-Prüfungen sind auf einmal pro Kalenderjahr begrenzt, sofern kein begründeter Anlass für eine zusätzliche Prüfung besteht. Die Kosten einer Vor-Ort-Prüfung trägt der Auftraggeber.

---

§ 9 Mitteilung bei Datenschutzverletzungen

1. Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO, die Daten des Auftraggebers betrifft.
2. Die Mitteilung enthält mindestens die in Art. 33 Abs. 3 DSGVO genannten Angaben, sofern diese dem Auftragnehmer zum Zeitpunkt der Mitteilung bereits vorliegen. Fehlende Angaben werden unverzüglich nachgereicht.

3. Der Auftragnehmer unterstützt den Auftraggeber bei einer ggf. erforderlichen Meldung an die zuständige Aufsichtsbehörde (Art. 33 DSGVO) und bei der Benachrichtigung betroffener Personen (Art. 34 DSGVO).

---

§ 10 Löschung und Rückgabe nach Vertragsende

1. Nach Beendigung des Hauptvertrags stellt der Auftragnehmer dem Auftraggeber eine **Datenexportfunktion** zur Verfügung, mit der dieser sämtliche von ihm in die Software eingegebenen Daten in maschinenlesbarem Format (CSV und JSON) herunterladen kann.
2. Während eines **Reaktivierungs- und Exportzeitraums von 90 Tagen** ab Vertragsende bleiben die Daten des Auftraggebers im System gespeichert. Eine reguläre Nutzung der Software ist in diesem Zeitraum nicht mehr möglich; der Datenexport sowie die Wiederaktivierung durch Abschluss eines neuen Hauptvertrags bleiben jedoch möglich.
3. Nach Ablauf dieses Zeitraums löscht der Auftragnehmer die Daten des Auftraggebers nach folgendem **Drei-Klassen-Modell**:

a. **Klasse A — vollständige Löschung**: Kunden- und Lieferantenstammdaten, Projekte, Angebote, Aufträge, Mitarbeitenden-Stammdaten, Zeiterfassungs- und Abwesenheitsdaten, Foto-Uploads, Tagebucheinträge sowie Anhänge werden vollständig und unwiderruflich gelöscht.

b. **Klasse B — gesetzliche Aufbewahrung**: Ausgestellte Rechnungen und unterzeichnete Protokolle unterliegen den gesetzlichen Aufbewahrungspflichten nach § 257 HGB und §§ 140, 147 AO (insbesondere zehn Jahre für Rechnungen). Diese Dokumente werden für die Dauer der Aufbewahrungspflicht in einem isolierten Archivbestand aufbewahrt und nach Ablauf gelöscht. Eine reguläre Verarbeitung findet nicht mehr statt.

c. **Klasse C — Audit-Protokoll**: Ein zusammenfassendes Lösch-Protokoll (Datum, Umfang, betroffene Datenkategorien) wird für Nachweiszwecke gemäß DSGVO-Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) gespeichert. Es enthält keine inhaltlichen personenbezogenen Daten der ursprünglich verarbeiteten Tätigkeit.

4. Auf gesonderte schriftliche Anforderung des Auftraggebers vor Ablauf des Reaktivierungszeitraums kann eine sofortige Löschung erfolgen, mit Ausnahme der unter Klasse B beschriebenen aufbewahrungspflichtigen Dokumente.

---

§ 11 Haftung

1. Für die Haftung der Parteien gelten die Regelungen der DSGVO, insbesondere Art. 82 DSGVO, sowie die Haftungsregelungen des Hauptvertrags.

2. Im Innenverhältnis haften die Parteien einander für Schäden im Verhältnis ihres Verursachungsbeitrags.

---

§ 12 Schlussbestimmungen

1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Anstelle der unwirksamen Bestimmung gilt diejenige als vereinbart, die dem wirtschaftlich Gewollten am nächsten kommt.
2. Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Dies gilt auch für die Abänderung dieser Klausel.
3. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gerichtsstand ist – soweit gesetzlich zulässig – der Sitz des Auftragnehmers.

Anlage 1 — Technische und organisatorische Maßnahmen (TOMs)

Der Auftragnehmer setzt zum Schutz der personenbezogenen Daten die nachfolgenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO um:

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

Zutrittskontrolle — Die Serverinfrastruktur wird ausschließlich bei einem zertifizierten Rechenzentrumsbetreiber innerhalb der Europäischen Union betrieben. Der physische Zugang ist nur autorisiertem Personal des Betreibers möglich und wird protokolliert.

Zugangskontrolle — Der Zugriff auf Systeme und Datenbanken erfolgt ausschließlich über verschlüsselte Verbindungen und mehrstufige Authentifizierungsverfahren. Passwörter werden mit modernen, dem aktuellen Stand der Technik entsprechenden Hashverfahren gespeichert.

Zugriffskontrolle — Innerhalb der Anwendung gilt ein rollenbasiertes Berechtigungsmodell. Daten verschiedener Auftraggeber sind auf logischer Ebene strikt voneinander getrennt; ein Datenzugriff über Mandantengrenzen hinweg ist technisch ausgeschlossen.

Trennungskontrolle — Produktions-, Test- und Backup-Umgebungen sind voneinander getrennt. Mandantendaten werden durch eindeutige Tenant-Identifier in jeder Datenbankabfrage isoliert.

Pseudonymisierung — Soweit für den Verarbeitungszweck möglich, werden personenbezogene Daten in Protokollen und technischen Logs pseudonymisiert verarbeitet.

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

Weitergabekontrolle — Sämtliche Datenübertragungen zwischen Anwendung, Datenbank und Endgeräten erfolgen verschlüsselt nach aktuellem Stand der Technik (Transportverschlüsselung).

Eingabekontrolle — Veränderungen an Datensätzen werden in der Anwendung mit Zeitstempel und Benutzerbezug nachvollziehbar gespeichert, soweit dies für den jeweiligen Datenbestand vorgesehen ist (z. B. Erstell- und Änderungszeitpunkte, Lösch-Protokolle).

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

Verfügbarkeitskontrolle — Tägliche, verschlüsselte Backups werden auf einem geografisch getrennten Speicher (innerhalb der EU) abgelegt. Die Wiederherstellbarkeit der Backups wird regelmäßig getestet.

Rasche Wiederherstellbarkeit — Im Schadensfall stehen dokumentierte Recovery-Prozeduren zur Verfügung.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Datenschutz-Management — Die getroffenen Maßnahmen werden mindestens jährlich auf ihre Wirksamkeit überprüft und an den jeweiligen Stand der Technik angepasst.

Incident-Response-Verfahren — Für den Fall einer Datenschutzverletzung sind Meldungs- und Reaktionspfade definiert (vgl. § 9 dieses Vertrags).

Auftragskontrolle — Bei der Auswahl und Beauftragung von Sub-Auftragsverarbeitern wird das Schutzniveau geprüft und vertraglich abgesichert (vgl. § 6 dieses Vertrags).

Anlage 2 — Liste der Sub-Auftragsverarbeiter

Folgende Sub-Auftragsverarbeiter werden zum Zeitpunkt des Vertragsschlusses eingesetzt:

Name & Anschrift	Leistung	Ort der Verarbeitung
IONOS SE, Elgendorfer Straße 57, 56410 Montabaur, Deutschland	Bereitstellung der Server-Infrastruktur (Hosting, Datenbank, Backup-Speicher) sowie Bereitstellung der Mail-Infrastruktur (Postfächer, ausgehender Mail-Versand)	Deutschland
Functional Software, Inc. d/b/a Sentry, 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA — Datenverarbeitung erfolgt in der EU-Region (Rechenzentrum Frankfurt). Übermittlungsgrundlage: EU-Standardvertragsklauseln nach Durchführungsbeschluss (EU)	Technisches Fehler-Monitoring (Error Tracking) zur Stabilitätssicherung der Anwendung	Verarbeitung in EU (Frankfurt); Vertragspartner mit Sitz in den USA

Name & Anschrift	Leistung	Ort der Verarbeitung
2021/914, enthalten im Data Processing Addendum 5.1.0 vom 29.05.2024.		

Hinweis zu Zahlungsdienstleistern: Die Mollie B.V. (Keizersgracht 313, 1016 EE Amsterdam, Niederlande) wird im Rahmen der Abwicklung der monatlichen Nutzungsvergütung tätig. Mollie verarbeitet die Zahlungsdaten gemäß eigener Datenschutzerklärung als **eigenständig Verantwortlicher** im Sinne der DSGVO und nicht als Auftragsverarbeiter des Auftragnehmers. Mollie ist daher kein Sub-Auftragsverarbeiter im Sinne dieses Vertrags.

Stand: [TT.MM.JJJJ] Version: 1.0