Vertrag zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO

Auftraggeber (Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO)

Firma	……
Anschrift	……
Vertreten durch	……

— nachfolgend „Auftraggeber" —

Auftragnehmer (Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO)

Firma	Novalytix UG (haftungsbeschränkt)
Anschrift	Richardstraße 88, 22089 Hamburg, Deutschland
Vertreten durch	N.A. van Duijn, Geschäftsführer
Handelsregister	Amtsgericht Hamburg, HRB 200478
USt-IdNr.	DE464336464
Kontakt Datenschutz	info.craft@novalytix.eu

— nachfolgend „Auftragnehmer" —

Präambel

Der Auftragnehmer stellt dem Auftraggeber die Software **CraftOS** als Software-as-a-Service zur Verfügung. Der Auftraggeber verwaltet damit seinen Handwerksbetrieb und verarbeitet dabei personenbezogene Daten seiner eigenen Kunden. Für diese Daten ist der Auftraggeber Verantwortlicher; der Auftragnehmer verarbeitet sie ausschließlich weisungsgebunden. Dieser Vertrag konkretisiert die Pflichten beider Parteien nach Art. 28 DSGVO.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der Bereitstellung von CraftOS.

(2) Die Laufzeit entspricht der Laufzeit des zugrunde liegenden Nutzungsvertrages. Eine Kündigung dieses AVV ohne gleichzeitige Beendigung des Nutzungsvertrages ist ausgeschlossen.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) **Zweck:** Betrieb, Bereitstellung, Wartung und Support von CraftOS.

(2) **Art der Verarbeitung:** Erheben, Erfassen, Speichern, Organisieren, Verändern, Auslesen, Abfragen, Verwenden, Übermitteln und Löschen im Rahmen der Funktionen der Software.

(3) **Kategorien betroffener Personen:**

- Kunden des Auftraggebers (Auftraggeber im handwerklichen Sinne)
- Ansprechpartner bei diesen Kunden
- Mitarbeiter und Mitwirkende des Auftraggebers, soweit sie Zugang zur Software haben

(4) **Kategorien personenbezogener Daten:**

- Stammdaten: Name, E-Mail-Adresse, Telefonnummer
- Anschriften: Rechnungsanschrift und Baustellenanschrift
- Freitextangaben in Notizfeldern
- Projekt- und Auftragsdaten, Aufgaben, Zeiterfassung, Materialpositionen
- Angebots- und Rechnungsdaten
- Baustellenfotos, auf denen Personen oder fremdes Eigentum erkennbar sein können
- Konto- und Zugangsdaten der Nutzer des Auftraggebers

(5) Der Auftraggeber entscheidet eigenverantwortlich, welche Daten er in die Software einstellt. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand dieses Vertrages; der Auftraggeber stellt sicher, dass er solche Daten nicht in die Software einstellt.

§ 3 Weisungsrecht

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die Nutzung der Software durch den Auftraggeber gilt als Weisung.

(2) Weisungen sind in Textform zu erteilen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Ausführung einer solchen Weisung auszusetzen.

(4) Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt.

§ 4 Vertraulichkeit

(1) Der Auftragnehmer verpflichtet alle zur Verarbeitung befugten Personen schriftlich zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie anpassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt eine allgemeine Genehmigung zur Hinzuziehung der in **Anlage 2** genannten Unterauftragsverarbeiter.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens **30 Tage** vor der Hinzuziehung eines weiteren oder der Ersetzung eines bestehenden Unterauftragsverarbeiters in Textform. Der Auftraggeber kann innerhalb dieser Frist

aus wichtigem datenschutzrechtlichem Grund widersprechen. Im Falle eines berechtigten Widerspruchs steht beiden Parteien ein Sonderkündigungsrecht zu.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Schutzniveau, das diesem Vertrag entspricht.

(4) Nebenleistungen ohne unmittelbaren Bezug zur Verarbeitung (etwa Telekommunikation oder Reinigung) gelten nicht als Unterauftragsverarbeitung.

§ 7 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber mit angemessenen Maßnahmen bei der Erfüllung von Betroffenenrechten nach Kapitel III DSGVO (Art. 15 bis 22).

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen und der vorherigen Konsultation.

§ 8 Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten **unverzüglich, spätestens innerhalb von 24 Stunden** nach Kenntniserlangung in Textform.

(2) Die Meldung enthält, soweit bekannt: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Gegenmaßnahmen.

(3) Die Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO obliegt dem Auftraggeber.

§ 9 Nachweis- und Kontrollrechte

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrages zur Verfügung.

(2) Der Auftraggeber ist berechtigt, die Einhaltung zu überprüfen — durch Selbstauskunft, durch Vorlage vorhandener Zertifikate oder Prüfberichte, oder durch Kontrolle vor Ort nach vorheriger Ankündigung mit angemessener Frist während der üblichen Geschäftszeiten.

(3) Kontrollen dürfen den Geschäftsbetrieb nicht unverhältnismäßig beeinträchtigen. Für über eine Kontrolle pro Kalenderjahr hinausgehende Prüfungen kann der Auftragnehmer eine angemessene Vergütung verlangen, es sei denn, ein konkreter Anlass besteht.

§ 10 Löschung und Rückgabe

(1) Nach Beendigung des Vertrages löscht der Auftragnehmer die Daten oder gibt sie nach Wahl des Auftraggebers zurück.

(2) Der Auftraggeber kann seine Daten während der Vertragslaufzeit und **innerhalb von 30 Tagen** nach Vertragsende exportieren. Nach Ablauf dieser Frist erfolgt die Löschung.

(3) Gesetzliche Aufbewahrungspflichten bleiben unberührt, insbesondere § 257 HGB und § 147 AO. Die betreffenden Daten werden für die Dauer der Aufbewahrungsfrist gesperrt und ausschließlich zu diesem Zweck verarbeitet.

§ 11 Haftung

Für die Haftung gelten Art. 82 DSGVO sowie die Regelungen des zugrunde liegenden Nutzungsvertrages.

§ 12 Schlussbestimmungen

(1) Änderungen bedürfen der Textform.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag gehen die Regelungen dieses Vertrages vor, soweit die Verarbeitung personenbezogener Daten betroffen ist.

(3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(4) Es gilt deutsches Recht.

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. VERTRAULICHKEIT

Zutrittskontrolle. Die Verarbeitung erfolgt ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland. Zutrittsschutz, Videoüberwachung und Zutrittsprotokollierung werden vom Rechenzentrumsbetreiber gewährleistet; eigene Serverräume unterhält der Auftragnehmer nicht.

Zugangskontrolle. Zugang zur Anwendung nur über persönliche Konten mit E-Mail und Passwort. Passwörter werden ausschließlich als Hash gespeichert (bcrypt). Administrativer Zugang zu den Servern ausschließlich über SSH mit Public-Key-Verfahren; Passwort-Authentifizierung ist deaktiviert.

Zugriffskontrolle. Mandantentrennung auf Anwendungsebene: jeder Datensatz ist einem Konto zugeordnet, und die Anwendung beschränkt jede Abfrage auf die Daten des angemeldeten Kontos. Zugriff auf Produktionssysteme ist auf die Geschäftsführung beschränkt.

Trennungskontrolle. Getrennte Datenbanken je Anwendung. Produktions- und Entwicklungsumgebungen sind getrennt; Entwicklungsumgebungen enthalten keine Produktionsdaten.

Verschlüsselung. Transportverschlüsselung durchgehend über TLS mit Zertifikaten von Let’s Encrypt; HTTP-Anfragen werden auf HTTPS umgeleitet. Datenbankverbindungen verlaufen ausschließlich über ein privates, nicht öffentlich erreichbares Netzwerk.

2. INTEGRITÄT

Eingabekontrolle. Änderungen an Datensätzen werden mit Zeitstempel versehen. Anwendungs- und Zugriffsprotokolle werden vorgehalten.

Weitergabekontrolle. Eine Übermittlung an Dritte erfolgt ausschließlich an die in Anlage 2 genannten Unterauftragsverarbeiter. Datenträger werden nicht versandt.

3. VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle. Tägliche Sicherung der Datenbank. Die Infrastruktur ist als Code beschrieben und reproduzierbar neu aufsetzbar. Unterbrechungsfreie Stromversorgung, Brandschutz und Klimatisierung werden vom Rechenzentrumsbetreiber gewährleistet.

Wiederherstellbarkeit. Wiederherstellung aus Sicherungen ist Bestandteil des Betriebskonzepts.

4. VERFAHREN ZUR ÜBERPRÜFUNG UND BEWERTUNG

Auftragskontrolle. Unterauftragsverarbeiter werden vertraglich nach Art. 28 DSGVO verpflichtet.

Datenschutzmanagement. Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO wird geführt. Sicherheitsrelevante Aktualisierungen werden zeitnah eingespielt; Abhängigkeiten werden automatisiert auf bekannte Schwachstellen geprüft.

Datenschutz durch Voreinstellung. Es werden nur die Datenfelder erhoben, die für den jeweiligen Vorgang erforderlich sind.

Anlage 2 — Unterauftragsverarbeiter

Unternehmen	Sitz	Leistung	Verarbeitete Daten
Hetzner Online GmbH	Deutschland	Hosting, Datenbank, Speicherung	sämtliche Anwendungsdaten
Mollie B.V.	Niederlande	Zahlungsabwicklung Abonnement	Abrechnungsdaten des Auftraggebers; keine Kundendaten des Auftraggebers
Brevo (Sendinblue SAS)	Frankreich	Versand von System-E-Mails	E-Mail-Adresse und Inhalt der jeweiligen Nachricht

Hinweis zu Brevo: Der E-Mail-Versand ist derzeit **nicht aktiv** (ActionMailer ist in CraftOS nicht konfiguriert). Der Eintrag ist vorsorglich aufgenommen und wird mit Aktivierung des Versands wirksam. Brevo verarbeitet innerhalb der EU; eine Übermittlung in ein Drittland findet nicht statt.

Unterschriften

Auftraggeber	**Auftragnehmer**
……	……
Ort, Datum	Ort, Datum
……	……
Name, Funktion	N.A. van Duijn, Geschäftsführer
	Novalytix UG (haftungsbeschränkt)

Dieses Dokument wurde als Entwurf erstellt und ist vor der Verwendung anwaltlich zu prüfen. Es ersetzt keine Rechtsberatung.