CRAFTBASE / RECHTLICHES

Auftragsverarbeitung (AVV)

Diese Vereinbarung regelt die Verarbeitung personenbezogener Kundendaten durch Craftbase und enthält die zugehörigen Angaben zu Verarbeitung, Schutzmaßnahmen und Unterauftragsverarbeitern.

Stand: 3. September 2026

1 Rollen, Parteien und Geltungsbereich

1.1 Diese Vereinbarung zur Auftragsverarbeitung (AVV) wird zwischen der Craftbase GmbH als dem im Impressum bezeichneten Anbieter und dem im Hauptvertrag bezeichneten Kunden geschlossen. Sie ergänzt den Hauptvertrag über die Nutzung von Craftbase.

1.2 Die AVV wird im Account oder zusammen mit einem individuellen Angebot elektronisch geschlossen. Craftbase dokumentiert die angenommene AVV-Fassung sowie Zeitpunkt, Unternehmen und handelnde Person; die angenommene Fassung bleibt für die Parteien abrufbar.

1.3 Die AVV gilt, soweit Craftbase personenbezogene Daten im Auftrag des Kunden verarbeitet. Sie erfasst entgeltliche Tarife, Testphasen und unentgeltliche Accounts ab dem Zeitpunkt, zu dem Craftbase erstmals personenbezogene Kundendaten im Auftrag verarbeitet.

1.4 Der Kunde handelt regelmäßig als Verantwortlicher. Verarbeitet der Kunde personenbezogene Daten seinerseits im Auftrag eines Dritten, handelt Craftbase im Anwendungsbereich dieser AVV als weiterer Auftragsverarbeiter; der Kunde gewährleistet, dass er Craftbase wirksam beauftragen und die erforderlichen Weisungen erteilen darf.

1.5 Für Verarbeitungen, bei denen Craftbase eigene Zwecke und Mittel festlegt, insbesondere die eigene Vertragsverwaltung, Abrechnung und gesetzlich erforderliche Sicherheits- oder Nachweisverarbeitung, handelt Craftbase nicht als Auftragsverarbeiter. Diese Verarbeitungen werden in der Datenschutzerklärung beschrieben.

1.6 Die Anlagen 1 bis 3 sind Bestandteil dieser AVV. Für die Auftragsverarbeitung geht diese AVV den AGB und der allgemeinen Leistungsbeschreibung vor; individuell ausgehandelte Datenschutzvereinbarungen bleiben vorrangig.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand der Verarbeitung ist die Bereitstellung, der Betrieb, die Absicherung, Wartung, Unterstützung und vertragsgemäße Weiterentwicklung der cloudbasierten Craftbase-Anwendung einschließlich der vom Kunden gebuchten oder aktivierten Funktionen.

2.2 Die Auftragsverarbeitung beginnt mit der erstmaligen Verarbeitung personenbezogener Kundendaten und besteht für die Dauer des Hauptvertrags einschließlich der vereinbarten Rückgabe-, Export- und Löschabwicklung.

2.3 Nach Ende des Hauptvertrags verarbeitet Craftbase noch vorhandene Kundendaten nur, soweit dies für den vereinbarten Export, die Löschung, die Sicherheit von Sicherungskopien, eine dokumentierte Weisung oder eine unmittelbar für Craftbase geltende gesetzliche Pflicht erforderlich ist.

2.4 Pflichten, die ihrem Zweck nach über das Vertragsende hinauswirken, insbesondere Vertraulichkeit, Schutz vorhandener Sicherungskopien, Rückgabe, Löschung und Nachweisführung, bleiben im erforderlichen Umfang bestehen.

3 Art und Zweck der Verarbeitung

3.1 Die Verarbeitung kann insbesondere das Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Übermitteln, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Sichern, Wiederherstellen, Exportieren und Löschen personenbezogener Daten umfassen.

3.2 Art und Zweck ergeben sich aus dem Hauptvertrag, der Leistungsbeschreibung, den gebuchten Funktionen, den administrativen Einstellungen und der bestimmungsgemäßen Nutzung durch den Kunden. Die Einzelheiten enthält Anlage 1.

3.3 Produktive KI-Funktionen verarbeiten Kundendaten nur durch aktive Nutzung oder Konfiguration durch einen berechtigten Nutzer. Beta- und Vorschaufunktionen setzen eine freiwillige Aktivierung voraus.

3.4 Craftbase verwendet Kundendaten nicht für eigene Werbung, Datenhandel oder zum Training eigener allgemein verfügbarer oder fremder Modelle. Ein KI-Dienstleister darf Kundendaten nur verarbeiten, wenn er nach dieser AVV wirksam einbezogen und in der aktuellen Unterauftragsverarbeiterliste genannt ist.

4 Dokumentierte Weisungen

4.1 Craftbase verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, soweit nicht Unionsrecht oder das Recht eines Mitgliedstaats Craftbase unmittelbar zu einer Verarbeitung verpflichtet.

4.2 Dokumentierte Weisungen ergeben sich aus Hauptvertrag, AVV, Leistungsbeschreibung, bestimmungsgemäßer Bedienung der Anwendung, administrativen Einstellungen sowie Mitteilungen über den Account, das Supportsystem oder in Textform.

4.3 Der Kunde benennt weisungsberechtigte Personen oder stellt deren Berechtigung über die Account- und Rollenverwaltung sicher. Craftbase darf die Berechtigung bei Zweifeln in angemessener Weise prüfen.

4.4 Ist Craftbase gesetzlich zu einer nicht angewiesenen Verarbeitung verpflichtet, informiert Craftbase den Kunden vorab über die betreffende Pflicht, soweit das anwendbare Recht diese Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

4.5 Hält Craftbase eine Weisung für datenschutzrechtswidrig, wird der Kunde ohne unangemessene Verzögerung informiert. Craftbase darf die betroffene Ausführung bis zur Klärung aussetzen, soweit keine unmittelbar erforderliche gesetzliche oder sicherheitsbedingte Maßnahme entgegensteht.

5 Rechte und Pflichten des Kunden

5.1 Der Kunde bleibt für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Rechte betroffener Personen und die Zulässigkeit seiner Weisungen verantwortlich. Er bestimmt innerhalb des vereinbarten Leistungsumfangs Zwecke und Mittel der Verarbeitung.

5.2 Der Kunde erfüllt insbesondere Informationspflichten, schafft erforderliche Rechtsgrundlagen und prüft die Voraussetzungen für besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten nach Art. 10 DSGVO.

5.3 Der Kunde verwaltet Nutzer, Rollen und Berechtigungen nach dem Erforderlichkeitsprinzip, schützt Zugangsdaten und informiert Craftbase ohne unangemessene Verzögerung über vermuteten Missbrauch oder kompromittierte Accounts.

5.4 Der Kunde stellt Craftbase die Informationen und Mitwirkung zur Verfügung, die zur vertragsgemäßen Verarbeitung, Bearbeitung von Anfragen, Eindämmung von Vorfällen und Erfüllung gesetzlicher Pflichten erforderlich sind.

5.5 Der Kunde kann im Rahmen dieser AVV Weisungen erteilen, Nachweise verlangen, Betroffenenanfragen veranlassen und die vereinbarten Kontrollrechte ausüben. Gesetzliche Rechte bleiben unberührt.

6 Pflichten von Craftbase

6.1 Craftbase verarbeitet Kundendaten nach dieser AVV, den dokumentierten Weisungen und dem anwendbaren Datenschutzrecht und gewährleistet, dass die mit der Verarbeitung betrauten Personen nur im zulässigen Umfang handeln.

6.2 Craftbase führt die für Auftragsverarbeiter erforderlichen Verzeichnisse von Verarbeitungstätigkeiten und stellt der zuständigen Aufsichtsbehörde die gesetzlich geschuldeten Informationen zur Verfügung.

6.3 Craftbase unterstützt den Kunden nach Maßgabe der Ziffern 11 bis 13 und informiert ihn über Umstände im eigenen Verantwortungsbereich, die dessen datenschutzrechtliche Pflichten wesentlich berühren.

6.4 Kopien und Vervielfältigungen von Kundendaten werden nur erstellt, soweit sie für Betrieb, Sicherheit, Wiederherstellung, Support oder die Erfüllung einer dokumentierten Weisung erforderlich sind.

6.5 Datenschutzbezogene Mitteilungen an Craftbase können an support@craftbase.de gerichtet werden. Ein Datenschutzbeauftragter wird in den Vertragsinformationen nur benannt, wenn eine entsprechende Bestellung und Zuständigkeit bestätigt sind.

7 Vertraulichkeit und Zugriffe

7.1 Craftbase verpflichtet alle Personen mit möglichem Zugriff auf Kundendaten vor dem Zugriff auf Vertraulichkeit oder stellt sicher, dass sie einer geeigneten gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung wirkt nach Ende ihrer Tätigkeit fort.

7.2 Zugriffe werden auf autorisierte Personen, erforderliche Aufgaben und den jeweils notwendigen Umfang begrenzt. Berechtigungen werden personenbezogen und rollenbezogen vergeben und bei Wegfall des Bedarfs entzogen.

7.3 Support- und Administrationszugriffe auf Kundeninhalte erfolgen nur anlassbezogen für Support, Wartung oder Sicherheit, werden sachlich und zeitlich begrenzt und soweit technisch vorgesehen nachvollziehbar protokolliert.

7.4 Muss Craftbase Kundendaten aufgrund einer vollziehbaren behördlichen oder gerichtlichen Anordnung offenlegen, wird der Kunde vorab informiert, soweit dies rechtlich zulässig ist, und die Offenlegung auf das rechtlich Erforderliche beschränkt.

8 Sicherheit der Verarbeitung

8.1 Craftbase trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der Risiken angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO.

8.2 Die für diesen Vertrag geltenden Kontrollbereiche und Maßnahmen sind in Anlage 2 beschrieben. Sicherheitskritische Betriebsdetails und Nachweise können zum Schutz der Systeme nur berechtigten Kunden, Prüfern und Behörden vertraulich bereitgestellt werden.

8.3 Craftbase darf Maßnahmen an die technische Entwicklung und veränderte Risiken anpassen, sofern das vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche schutzmindernde Änderungen bedürfen einer gesonderten rechtlichen Grundlage.

8.4 Craftbase unterhält Verfahren, um die Wirksamkeit der Maßnahmen risikoorientiert zu überprüfen und festgestellte wesentliche Schwächen angemessen zu behandeln. Konkrete Prüfintervalle gelten nur, wenn sie ausdrücklich dokumentiert sind.

8.5 Die Sicherheitsbeiträge des Kunden, insbesondere sichere Endgeräte, angemessene Rollenvergabe und Schutz der Zugangsdaten, ergänzen die Maßnahmen von Craftbase, verlagern aber keine gesetzlichen Pflichten von Craftbase auf den Kunden.

9 Unterauftragsverarbeiter

9.1 Der Kunde erteilt Craftbase eine allgemeine schriftliche Genehmigung, die in Anlage 3 aufgeführten Unterauftragsverarbeiter für die dort beschriebenen Leistungen einzusetzen.

9.2 Craftbase veröffentlicht die aktuelle Unterauftragsverarbeiterliste als Bestandteil dieser AVV und hält frühere operative Listenstände nachvollziehbar vor.

9.3 Craftbase informiert den administrativen Kundenkontakt grundsätzlich mindestens 30 Kalendertage vor dem beabsichtigten Einsatz eines neuen oder ersetzten Unterauftragsverarbeiters per E-Mail und aktualisiert die öffentliche Liste.

9.4 Der Kunde kann innerhalb der Ankündigungsfrist aus konkreten, nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Ein Widerspruch gegen beliebige Änderungen ohne Bezug zum Schutz personenbezogener Daten ist nicht ausreichend.

9.5 Die Parteien prüfen zunächst eine zumutbare Alternative oder Konfiguration. Ist keine angemessene Lösung verfügbar, kann jede Partei den von der Änderung betroffenen Dienst mit angemessener Frist beenden; weitergehende Rechte aus Hauptvertrag und zwingendem Recht bleiben unberührt.

9.6 Erfordert ein Sicherheits- oder Notfall einen kurzfristigeren Wechsel, darf Craftbase die Frist auf das erforderliche Maß verkürzen und informiert den Kunden mit Begründung so früh wie möglich.

9.7 Craftbase verpflichtet jeden Unterauftragsverarbeiter mindestens zu gleichwertigen Datenschutzpflichten und bleibt dem Kunden für dessen vertragsgemäße Leistung nach Art. 28 Abs. 4 DSGVO verantwortlich.

10 Internationale Übermittlungen

10.1 Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgen nur auf dokumentierte Weisung des Kunden oder aufgrund einer unmittelbar für Craftbase geltenden gesetzlichen Pflicht und unter Einhaltung von Kapitel V DSGVO.

10.2 Als Übermittlung gilt auch ein rechtlich relevanter Fernzugriff aus einem Drittland. Die aktuelle Anlage 3 beschreibt die bekannten Verarbeitungsorte und die für den jeweiligen Dienst herangezogenen Schutzmechanismen.

10.3 Soweit erforderlich, verwendet Craftbase insbesondere einen Angemessenheitsbeschluss oder geeignete Garantien wie die jeweils anwendbaren EU-Standardvertragsklauseln und berücksichtigt notwendige Transferprüfungen und ergänzende Maßnahmen.

10.4 Eine für regional konfigurierbare Kerndaten gewählte Region in Deutschland begründet keine pauschale Zusage, dass sämtliche Daten, Metadaten, Supportvorgänge oder Unterauftragsverarbeitungen ausschließlich in Deutschland stattfinden.

11 Unterstützung bei Betroffenenrechten

11.1 Craftbase unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung durch vorhandene Such-, Auskunfts-, Export-, Berichtigungs-, Einschränkungs- und Löschmöglichkeiten sowie durch angemessene ergänzende Hilfe bei Betroffenenanfragen.

11.2 Der Kunde prüft Identität, Rechtsgrundlage, Reichweite und Ausnahmen einer Betroffenenanfrage und bleibt für deren fristgerechte Beantwortung verantwortlich.

11.3 Geht eine erkennbar auf Kundendaten bezogene Anfrage unmittelbar bei Craftbase ein, leitet Craftbase sie ohne eigene Sachentscheidung und ohne unangemessene Verzögerung sicher an den zuständigen Kundenkontakt weiter, soweit keine gesetzliche Pflicht zur unmittelbaren Bearbeitung besteht.

11.4 Soweit der Kunde die zur Bearbeitung erforderlichen Daten nicht selbst über die Anwendung abrufen kann, stellt er Craftbase eine hinreichend bestimmte dokumentierte Weisung und die zur Identifizierung erforderlichen Informationen bereit.

12 Datenschutzverletzungen und weitere Unterstützung

12.1 Craftbase meldet dem Kunden eine Verletzung des Schutzes personenbezogener Kundendaten im eigenen Verantwortungsbereich ohne unangemessene Verzögerung nach Bekanntwerden.

12.2 Die Erstmeldung enthält, soweit verfügbar, eine Beschreibung des Vorfalls, betroffene Daten und Personengruppen, mögliche Folgen, ergriffene oder vorgeschlagene Maßnahmen und einen Ansprechpartner. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

12.3 Craftbase trifft angemessene Maßnahmen zur Eindämmung, Untersuchung, Beweissicherung und Vermeidung vergleichbarer Vorfälle und unterstützt den Kunden mit den verfügbaren Informationen bei dessen Risikobewertung.

12.4 Der Kunde entscheidet grundsätzlich über Meldungen an Aufsichtsbehörden und Benachrichtigungen betroffener Personen. Craftbase kommuniziert zu Kundendaten nur auf dokumentierte Weisung oder aufgrund einer eigenen zwingenden gesetzlichen Pflicht.

12.5 Craftbase unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei dessen Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Sicherheit, Meldungen, Benachrichtigungen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

12.6 Übliche Unterstützung durch Produktfunktionen, Dokumentation und Standardauskünfte ist mit dem SaaS-Entgelt abgegolten. Außergewöhnlicher kundenspezifischer Aufwand kann nach vorheriger Information und Abstimmung berechnet werden; gesetzlich geschuldete Basishilfe bleibt unberührt.

13 Nachweise und Prüfungen

13.1 Craftbase stellt dem Kunden die Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind, und wirkt an gesetzlich erforderlichen Prüfungen mit.

13.2 Nachweise werden vorrangig durch diese AVV, die TOM-Dokumentation, die Unterauftragsverarbeiterliste, standardisierte Auskünfte und vorhandene geeignete Prüfberichte erbracht.

13.3 Reichen diese Nachweise für berechtigte Fragen nicht aus, kann der Kunde selbst oder durch einen unabhängigen fachkundigen Prüfer ergänzende Prüfungen durchführen. Sie sind angemessen anzukündigen, auf den erforderlichen Umfang zu begrenzen und grundsätzlich während üblicher Geschäftszeiten durchzuführen.

13.4 Ohne konkreten Anlass ist grundsätzlich eine Kundenprüfung pro Kalenderjahr vorgesehen. Zusätzliche Prüfungen bleiben bei einem erheblichen Vorfall, begründetem Verdacht, wesentlicher Änderung oder behördlicher Anordnung möglich.

13.5 Prüfer sind auf Vertraulichkeit zu verpflichten. Daten anderer Kunden, Geschäftsgeheimnisse, Quellcode und sicherheitskritische Informationen werden nur offengelegt, soweit dies gesetzlich erforderlich ist und kein gleichwertiger Nachweis genügt.

13.6 Jede Partei trägt grundsätzlich ihre eigenen Prüfungskosten. Außergewöhnlichen Zusatzaufwand stimmt Craftbase vorab mit dem Kunden ab; bei einem nachgewiesenen wesentlichen Verstoß von Craftbase werden die erforderlichen Nachweiskosten nicht auf den Kunden verlagert.

14 Rückgabe, Export und Löschung

14.1 Während der Vertragslaufzeit kann der Kunde die jeweils produktiv unterstützten Export- und Löschfunktionen nutzen. Kundenspezifische Formate oder zusätzliche Datenaufbereitung sind nur geschuldet, wenn sie gesondert vereinbart wurden.

14.2 Nach Ende eines entgeltlichen Hauptvertrags erhält der Kunde für 30 Kalendertage einen eingeschränkten Lese- und Exportzugriff. Der Kunde sichert innerhalb dieses Zeitraums die von ihm benötigten Daten und Dokumente.

14.3 Eine Rückgabe erfolgt grundsätzlich über die unterstützten Exporte. Abweichende dokumentierte Weisungen werden umgesetzt, soweit sie rechtlich zulässig, technisch möglich und vom vereinbarten Leistungsumfang umfasst sind.

14.4 Nach Ablauf des Exportzeitraums löscht oder anonymisiert Craftbase Kundendaten aus den Produktivsystemen nach dem dokumentierten Löschverfahren. Dies umfasst grundsätzlich auch vom Kunden ausgestellte Rechnungen und sonstige Dokumente, sofern keine gesonderte Aufbewahrung beauftragt ist oder eine unmittelbar für Craftbase geltende Pflicht entgegensteht.

14.5 Gesetzliche Aufbewahrungspflichten des Kunden begründen für sich allein keine eigene Aufbewahrungsbefugnis von Craftbase nach Vertragsende. Eine fortgesetzte Aufbewahrung im Auftrag erfordert eine dokumentierte Weisung und eine entsprechende vertragliche Grundlage.

14.6 In Sicherungskopien verbleibende Daten werden nur für Wiederherstellung und Sicherheit verarbeitet und nach den technisch festgelegten Sicherungszyklen überschrieben. Werden Sicherungen wiederhergestellt, gelten die Lösch- und Sperrvorgaben erneut.

14.7 Craftbase bestätigt dem Kunden auf Anfrage in angemessener Form den Abschluss des regulären Löschprozesses. Gesetzlich zulässige oder erforderliche Restverarbeitungen werden auf den jeweiligen Zweck beschränkt.

15 Haftung, Beendigung und Schlussbestimmungen

15.1 Die Haftung zwischen den Parteien richtet sich nach Art. 82 DSGVO, sonstigem zwingendem Recht und den rechtlich freigegebenen Haftungsregelungen des Hauptvertrags. Rechte betroffener Personen und Befugnisse der Aufsichtsbehörden werden durch diese AVV nicht beschränkt.

15.2 Bei einem wesentlichen behebbaren Verstoß gegen diese AVV kann die andere Partei zunächst Abhilfe innerhalb angemessener Frist verlangen. Bleibt der Verstoß bestehen oder ist ein Abwarten unzumutbar, kann der betroffene Dienst aus wichtigem Grund beendet werden.

15.3 Die Beendigung des Hauptvertrags beendet auch diese AVV, soweit nicht Vertraulichkeit, Rückgabe, Löschung, Schutz von Sicherungskopien und Nachweise ihrem Zweck nach fortgelten.

15.4 Materielle Änderungen dieser AVV werden aktiv zwischen den Parteien vereinbart. Redaktionelle Klarstellungen und ausschließlich schutzverstärkende Anpassungen können dokumentiert mitgeteilt werden, ohne laufende Rechte rückwirkend zu verändern.

15.5 Änderungen der TOMs sind ohne erneute Zustimmung zulässig, wenn das vereinbarte Schutzniveau insgesamt erhalten bleibt. Änderungen der Unterauftragsverarbeiterliste folgen ausschließlich dem Verfahren nach Ziffer 9.

15.6 Es gilt die im Hauptvertrag vereinbarte Rechtsordnung und, soweit wirksam vereinbart, dessen Gerichtsstand. Zwingende datenschutzrechtliche Zuständigkeiten bleiben unberührt.

15.7 Sollte eine Bestimmung dieser AVV unwirksam oder undurchführbar sein, bleiben die übrigen Bestimmungen wirksam. An die Stelle der betroffenen Regelung tritt das anwendbare Gesetz.

15.8 Die deutsche Fassung dieser AVV ist allein verbindlich. Die englische Fassung und andere Übersetzungen dienen ausschließlich der Information; bei Abweichungen geht die deutsche Fassung vor.

Anlage 1 Beschreibung der Verarbeitung

A1.1 Diese Anlage konkretisiert Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie Datenarten und Kategorien betroffener Personen. Maßgeblich sind nur die vom Kunden tatsächlich genutzten Funktionen.

A1.2 Der Kunde darf besondere Kategorien personenbezogener Daten nur im vorgesehenen Umfang und bei Vorliegen der gesetzlichen Voraussetzungen verarbeiten. Craftbase erhält dadurch keine Befugnis, diese Daten für eigene Zwecke zu verwenden.

A1.3 Ändert sich der gebuchte Funktionsumfang, gilt diese Anlage für die dadurch bestimmungsgemäß hinzukommenden Verarbeitungsvorgänge, soweit keine materielle Änderung der AVV erforderlich ist.

Rahmen der Verarbeitung

Gegenstand	Bereitstellung, Betrieb, Sicherheit, Wartung, Support und vertragsgemäße Weiterentwicklung der Craftbase-SaaS-Anwendung.
Zwecke	Digitale Organisation von Kunden-, Projekt-, Auftrags-, Planungs-, Arbeitszeit-, Kommunikations-, Dokumentations- und Abrechnungsprozessen des Kunden.
Dauer	Laufzeit des Hauptvertrags einschließlich vereinbarter Export- und Löschabwicklung sowie technisch erforderlicher Sicherungszyklen.

Datenarten

Stamm- und Kontaktdaten	Namen, geschäftliche Kontaktdaten, Anschriften, Ansprechpartner sowie Kunden-, Lieferanten- und Projektzuordnungen.
Nutzer- und Beschäftigtendaten	Account-, Authentifizierungs-, Rollen-, Berechtigungs-, Arbeitszeit-, Zeitkonto-, Urlaubs- und Abwesenheitsdaten.
Projekt- und Auftragsdaten	Projekte, Baustellen, Aufgaben, Termine, Leistungen, Materialien, Status, Berichte, Abnahmen und individuelle Felder.
Kommunikation und Dateien	Nachrichten, Notizen, Fotos, Anhänge, Pläne, Nachweise und sonstige vom Kunden eingestellte Inhalte.
Geschäfts- und Dokumentdaten	Angebote, Rechnungen, Zahlungsbezüge, Dokumentvorlagen, Korrekturen, Exporte und zugehörige Verlaufsinformationen.
Nutzungs- und Sicherheitsdaten	Technische Nutzungs-, Geräte-, Zugriffs-, Fehler-, Änderungs-, Sicherheits- und Protokolldaten, soweit sie im Auftrag verarbeitet werden.

Kategorien betroffener Personen

Betriebsangehörige	Beschäftigte, Geschäftsleitung, Auszubildende einschließlich Minderjähriger, Praktikanten, freie Mitarbeitende und sonstige Nutzer des Kunden.
Geschäftskontakte	Kunden, Interessenten, Lieferanten, Nachunternehmer, Geschäftspartner und deren Ansprechpartner.
Projektbeteiligte	Bauherren, Planer, Bauleitungen, Projektkontakte und weitere Personen, deren Daten der Kunde einem Auftrag oder Projekt zuordnet.
Weitere Personen	Sonstige Personen, deren Daten der Kunde im Rahmen der bestimmungsgemäßen Nutzung rechtmäßig in Craftbase erfasst.

Besondere Daten und Begrenzungen

Gesundheitsbezug	Die vorgesehene Abwesenheitsart Krankheit kann einen begrenzten Gesundheitsbezug enthalten. Diagnosen und medizinische Detailangaben sind nicht bestimmungsgemäß vorgesehen.
Weitere Art.-9-Daten	Andere besondere Kategorien sind ohne ausdrückliche Vereinbarung, geeignete Funktion und bestätigte Schutzmaßnahmen nicht bestimmungsgemäß vorgesehen.
Art.-10-Daten	Daten über strafrechtliche Verurteilungen und Straftaten sind ohne ausdrückliche Vereinbarung und bestätigte Schutzmaßnahmen nicht bestimmungsgemäß vorgesehen.
Standortdaten	GPS- oder vergleichbare Standortdaten sind erst erfasst, wenn eine konkrete aktivierte Produktfunktion ihre Verarbeitung vorsieht und dokumentiert ist.

Anlage 2 Technische und organisatorische Maßnahmen

A2.1 Die folgenden Kontrollbereiche beschreiben das vertraglich geschuldete Schutzniveau. Craftbase setzt die Maßnahmen risikoorientiert und entsprechend der jeweils eingesetzten technischen Architektur um.

A2.2 Einzelne Maßnahmen können durch gleichwertige oder wirksamere Maßnahmen ersetzt werden. Das Schutzniveau darf dadurch insgesamt nicht unterschritten werden.

A2.3 Weitergehende technische Nachweise, Konfigurationen und Prüfunterlagen werden berechtigten Empfängern vertraulich bereitgestellt, soweit dies zum Nachweis erforderlich und mit dem Schutz der Systeme vereinbar ist.

Datenschutzorganisation und Vertraulichkeit

Verantwortung	Zuständigkeiten für Datenschutz und Informationssicherheit werden festgelegt und wesentliche Verarbeitungsvorgänge dokumentiert.
Personal	Berechtigte Personen werden vor Zugriff auf Vertraulichkeit verpflichtet und für ihre Aufgaben angemessen sensibilisiert.

Physischer Schutz und Cloud-Infrastruktur

Infrastruktur	Produktive Systeme werden über geeignete Cloud-Infrastruktur betrieben; der physische Schutz der Rechenzentren wird vertraglich auf den Infrastrukturbetreiber übertragen und überprüfbar gemacht.
Arbeitsumgebung	Zugriffe aus Arbeitsumgebungen werden durch organisatorische und technische Vorgaben auf autorisierte Personen und Geräte begrenzt.

Identitäts- und Zugriffskontrolle

Authentisierung	Zugänge sind personenbezogen; Authentisierungs- und Schutzmechanismen werden dem Risiko und der jeweiligen administrativen Berechtigung angepasst.
Berechtigungen	Rollen und Rechte folgen dem Erforderlichkeitsprinzip und werden bei Aufgabenwechsel oder Wegfall des Bedarfs angepasst oder entzogen.

Mandantentrennung und Datenzugriff

Trennung	Kundendaten werden logisch nach Mandanten und Berechtigungen getrennt; Zugriffe werden im vorgesehenen Anwendungskontext geprüft.
Support	Support- und Administrationszugriffe sind anlassbezogen, auf das Erforderliche begrenzt und soweit technisch vorgesehen nachvollziehbar protokolliert.

Übertragung und Speicherung

Übertragungsschutz	Personenbezogene Daten werden bei der Übertragung durch dem Risiko angemessene technische Schutzmechanismen gegen unbefugte Kenntnisnahme und Veränderung abgesichert.
Speicherschutz	Speicher, Zugänge und administrative Schnittstellen werden entsprechend Schutzbedarf und technischer Architektur abgesichert; konkrete Verfahren werden in der vertraulichen Sicherheitsdokumentation nachgewiesen.

Protokollierung und Vorfallbehandlung

Nachvollziehbarkeit	Sicherheitsrelevante administrative und technische Ereignisse werden im vorgesehenen Umfang erfasst und vor unbefugter Veränderung geschützt.
Vorfälle	Erkannte Sicherheitsvorfälle werden bewertet, eingedämmt, dokumentiert und nach dem festgelegten Melde- und Eskalationsprozess behandelt.

Verfügbarkeit, Sicherung und Wiederherstellung

Verfügbarkeit	Betriebs- und Wiederherstellungsmaßnahmen werden nach Risiko und vereinbartem Leistungsumfang ausgestaltet; eine feste Verfügbarkeits- oder Wiederherstellungszeit gilt nur bei ausdrücklicher Vereinbarung.
Sicherungen	Erforderliche Sicherungskopien werden geschützt, zweckgebunden verarbeitet und nach den technisch dokumentierten Zyklen überschrieben; Wiederherstellungsverfahren werden angemessen überprüft.

Entwicklung, Änderungen und Dienstleister

Software-Lebenszyklus	Sicherheits- und Datenschutzanforderungen werden bei Entwicklung, Prüfung, Bereitstellung und Änderung risikoorientiert berücksichtigt; festgestellte relevante Schwächen werden angemessen behandelt.
Dienstleister	Unterauftragsverarbeiter werden vor Einsatz datenschutz- und sicherheitsbezogen geprüft, vertraglich gebunden und entsprechend ihrem Risiko überwacht.

Anlage 3 Unterauftragsverarbeiter und Übermittlungsinformationen

A3.1 Diese Anlage führt die für die Auftragsverarbeitung bestätigten Unterauftragsverarbeiter auf. Ein Dienst darf Kundendaten im Auftrag erst verarbeiten, wenn seine Rolle, Leistung und erforderlichen Übermittlungsinformationen geprüft und dokumentiert sind.

A3.2 Änderungen werden nach Ziffer 9 angekündigt und mit einem neuen datierten Listenstand veröffentlicht. Frühere operative Listenstände bleiben als Nachweis erhalten.

A3.3 Die Angaben zu Regionen beziehen sich nur auf die jeweils regional konfigurierbaren Dienste. Abweichende Support-, Metadaten- oder weitere Unterauftragsverarbeitungen richten sich nach den dienstbezogenen Vertrags- und Übermittlungsinformationen.

Google Cloud und Firebase

Dienstleister	Google Cloud und Firebase-Dienste.
Leistungen	Cloud-Infrastruktur, Firebase Authentication, Firebase Data Connect und weitere tatsächlich konfigurierte Google- oder Firebase-Betriebsdienste.
Zweck	Hosting, Datenverarbeitung, Authentifizierung, Betrieb, Sicherheit, Fehlerbehandlung und technische Unterstützung der Craftbase-Anwendung.
Daten	Kundendaten nach Anlage 1 sowie technische Account-, Authentifizierungs-, Nutzungs-, Sicherheits- und Protokolldaten, abhängig vom eingesetzten Dienst.
Verarbeitungsorte	Deutschland, insbesondere Frankfurt, für entsprechend regional konfigurierte Kerndaten; einzelne Dienste, Supportvorgänge und weitere Unterauftragsverarbeiter können andere Orte einbeziehen.
Übermittlungsgrundlage	Für Verarbeitungen außerhalb des EWR gelten die für den jeweiligen Dienst wirksam vereinbarten Mechanismen nach Kapitel V DSGVO.