CATHAGO

Auftragsverarbeitungsvereinbarung

gemäß Art. 28 DSGVO

zwischen

[Kunde]

[Adresse]

als Verantwortliche/r

– nachfolgend „**Auftraggeber**“ genannt –

und

CATHAGO Technology UG (haftungsbeschränkt)

Hessische Straße 11
10115 Berlin
Deutschland

als Auftragsverarbeiter/in

– nachfolgend „**Auftragnehmer**“ genannt –

– nachfolgend jeder auch „Partei“ und gemeinsam „Parteien“ –

Präambel

Der Auftragnehmer hat mit dem Auftraggeber einen Nutzungsvertrag über die Nutzung der CATHAGO Software geschlossen (im Folgenden: „**Hauptvertrag**“). Teil der Durchführung des Hauptvertrages ist die Verarbeitung von personenbezogenen Daten des Auftraggebers im Sinne der EU Datenschutz-Grundverordnung („**DSGVO**“). Zur Erfüllung der Anforderungen der DSGVO, insbesondere des Art. 28 Abs. 3 DSGVO, schließen die Parteien die nachfolgende Vereinbarung.

1. Gegenstand/Umfang und Dauer der Beauftragung

1.1 Im Rahmen der Erbringung der gemäß dem Hauptvertrag durchzuführenden Leistungen, erlangt der Auftragnehmer Zugriff auf die personenbezogenen Daten des Auftraggebers (im Folgenden: „**Auftraggeberdaten**“). Diese darf er ausschließlich im Auftrag und nach Weisung des Auftraggebers verarbeiten.

1.2 Art, Umfang und Zweck der Verarbeitung von Auftraggeberdaten durch den Auftragnehmer sowie die von dieser Verarbeitung betroffenen Kategorien betroffener Personen sind in **Anlage 1** spezifiziert. Ein über die in **Anlage 1** beschriebene Verarbeitung hinausgehender Umgang mit Auftraggeberdaten ist dem Auftragnehmer untersagt.

1.3 Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

1.4 Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen. Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland.

1.5 Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit den Auftraggeberdaten in Berührung kommen.

1.6 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Die Möglichkeit zur fristlosen Kündigung aus einem wichtigen Grund bleibt hiervon unberührt.

2. Weisungsbefugnisse des Auftraggebers

2.1 Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art und Umfang der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "**Weisungsrecht**"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

2.2 Weisungen werden vom Auftraggeber grundsätzlich schriftlich erteilt; mündlich erteilte Weisungen sind vom Auftraggeber schriftlich zu bestätigen. Die weisungs- und empfangsberechtigten Personen ergeben sich aus **Anlage 2**, sofern im Hauptvertrag keine eigene Regelung getroffen wurde.

2.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er dies dem Auftraggeber mitzuteilen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis der Auftraggeber diese bestätigt oder ändert.

2.4 Der Auftraggeber hat den Auftragnehmer gleichsam unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3. Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat bei der Verarbeitung der Auftraggeberdaten 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. Die konkret durch den Auftragnehmer implementierten technisch-organisatorischen Maßnahmen ergeben sich aus **Anlage 3**.

3.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

3.3 Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in **Anlage 3** bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise demonstrieren.

3.4 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

3.5 Der Auftraggeber stellt sicher, dass die aus Art. 32 DSGVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

4. Informations- und Unterstützungspflichten des Auftragnehmers

4.1 Im Falle einer Verletzung des Schutzes der Auftraggeberdaten i.S. Art. 33 DSGVO durch den Auftragnehmer, durch bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 24 Stunden in Schriftform oder elektronischer Form hierüber informieren.

4.2 Der Auftragnehmer wird den Auftraggeber im Falle der Ziffer 4.1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen im Rahmen des Zumutbaren unterstützen und ihm die hierfür erforderlichen Informationen zur Verfügung stellen.

4.3 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Datenschutz-Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

4.4 Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde wird der Auftragnehmer dem Auftraggeber unverzüglich, nachdem er Kenntnis von der beabsichtigten Durchführung dieser Prüfung erlangt hat, mitteilen, sofern die Verarbeitungsvorgänge für den Auftraggeber betroffen sind.

4.5 Der Auftragnehmer unterstützt den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen

vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO soweit dies erforderlich ist.

5. Sonstige Verpflichtungen des Auftragnehmers

5.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

5.2 Der Auftragnehmer wird die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO sicherstellen. Er sichert zu, im Umgang mit Auftraggeberdaten nur Beschäftigte einzusetzen, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie durch Unionsrecht oder das Recht der Mitgliedstaaten gesetzlich zur Verarbeitung verpflichtet sind.

5.3 Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Die Kontaktdaten des Datenschutzbeauftragten sind:

Stephan Menzemer
E-Mail: datenschutz@cathago.de

6. Unterauftragsverarbeitung

6.1 Als Unterauftragsverarbeitung im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

6.2 Der Auftraggeber genehmigt die in **Anlage 4** genannten Unterauftragnehmer.

6.3 Der Wechsel bestehender oder die Beauftragung neuer Unterauftragnehmer sind nur zulässig, (i) soweit der Auftragnehmer einen solchen Wechsel oder eine solche neue Beauftragung dem Auftraggeber mindestens 30 Tage vor Beginn der Unterauftragsverarbeitung schriftlich oder in Textform anzeigt und (ii) soweit der Auftraggeber bis zu diesem Zeitpunkt keinen Einspruch gegen den geplanten Wechsel oder die geplante Beauftragung einlegt.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, erfolgt dies nur nach vorheriger Anzeige gegenüber dem Auftraggeber und nur soweit die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO zur Gewährleistung eines angemessenen Sicherheitsniveaus erfüllt sind.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach dieser Vereinbarung und nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung innerhalb einer angemessenen Frist die für die Durchführung der Kontrollen erforderlichen Auskünfte und Nachweise zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.2 Der Auftraggeber hat das Recht, bei berechtigten Zweifeln an der Einhaltung dieser Vereinbarung durch den Auftragnehmer Vor-Ort Überprüfungen durchzuführen oder durch einen im Einzelfall zu benennenden Prüfer durchführen zu lassen. Diese Überprüfungen erfolgen stets in Abstimmung mit dem Auftragnehmer und sind mit angemessenem Vorlauf anzukündigen, um den Geschäftsbetrieb des Auftragnehmers nicht unverhältnismäßig zu stören.

7.3 Werden bei einer solchen Überprüfung Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

7.4 Der Nachweis geeigneter technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz) erfolgen.

8. Rechte der Betroffenen

8.1 Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO.

8.2 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und dessen Weisungen abwarten. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person aktiv in Kontakt treten.

9. Löschung und Rückgabe von personenbezogenen Daten

9.1 Kopien oder Duplikate der Auftraggeberdaten werden ohne Wissen des Auftraggebers 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.

9.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, soweit möglich, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung dieser personenbezogenen Daten besteht. Ausgenommen von dieser Regelung sind Datenbestände in Backups und sonstigen zur Wiederherstellung bestimmten Systemen.

9.3 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

10. Haftung

10.1 Die Haftung der Parteien richtet sich nach dem Hauptvertrag.

10.2 Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Dies gilt auch im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

11. Schlussbestimmungen

11.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

11.2 Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

11.3 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

11.4 Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

11.5 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Berlin.

Unterschriften

Ort/Datum:

Auftragnehmer, vertreten durch
Geschäftsführer Emil Buxmann

Ort/Datum:

Auftraggeber

Anlage 1 – Beschreibung der Verarbeitung

Art der Daten	Zweck der Datenverarbeitung	Kreis der betroffenen Personen
Kundenstammdaten (Name, Vorname, E-Mail, Telefon, Mobil, Funktion)	Speichern und verwenden der Daten zur Bereitstellung der Zugangsdaten für die Softwarenutzung und Darstellung der Mitarbeiter im Bauunternehmen	Mitarbeiter des Auftraggebers
Logistik Stammdaten (Name, Vorname, E-Mail, Telefon, Mobil)	Speichern und verwenden der Daten zur Bereitstellung der Zugangsdaten für den Logistikanbieter	Logistiker
Lieferantenstammdaten (Name, Vorname, Telefon, Mobil, E-Mail, Adresse, Geburtsdatum, Firma)	Speichern und verwenden der Daten zur Bereitstellung der Zugangsdaten für die Softwarenutzung und Darstellung der Lieferanten	Lieferant
Zuweiserstammdaten (Name, Vorname, E-Mail, Telefon, Mobil)	Speichern und verwenden der Daten zur Bereitstellung der Zugangsdaten für die Softwarenutzung	Zuweiser

Es werden keine besonderen Kategorien von personenbezogenen Daten im Sinne des Art. 9 DSGVO verarbeitet.

Anlage 2 – Weisungs- und empfangsberechtigte Personen

Folgende Person(en) ist/sind beim Auftraggeber berechtigt, Weisungen hinsichtlich der diesem Auftragsverarbeitungsvertrag gegenständlichen Datenverarbeitung zu erteilen:

Name:

Erreichbarkeit innerhalb des Unternehmens:

Folgende Person(en) ist/sind beim Auftragnehmer berechtigt, Weisungen hinsichtlich der diesem Auftragsverarbeitungsvertrag gegenständlichen Datenverarbeitung entgegenzunehmen:

Name: Emil Buxmann

Erreichbarkeit innerhalb des Unternehmens:

E-Mail: emil.buxmann@cathago.de

Tel.: 0170 738 608 1

Anlage 3 – Technisch-organisatorische Maßnahmen

Anlage 3 finden Sie unter der folgenden Landing Page: https://security.cathago.de/

Anlage 4 – Unterauftragnehmer

Anlage 4 finden Sie unter der folgenden Landing Page: https://security.cathago.de/