Vereinbarung zur Auftragsverarbeitung

Bitte senden Sie den Vertrag per E-Mail an datenschutz@copago.de oder per Post in zweifacher Ausführung an u.g. Anschrift unterzeichnet zurück.

zwischen

Firma, Straße, Hausnr., PLZ, Ort, Land

gesetzlich vertreten durch

Vorname, Name des Vertreters

– Verantwortlicher - nachfolgend „**Auftraggeber**" genannt,

und

der copago AG, Zum Aquarium 6a, 46047 Oberhausen,

gesetzlich vertreten durch die copago AG, ebenda, diese gesetzlich vertreten durch den Vorstand Dominik Skora und Karl-Heinz Faulhaber, ebenda,

– Auftragsverarbeiter - nachfolgend „**Auftragnehmer**" genannt.

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(5) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Kassensoftware auf Grundlage des Vertrags vom [ ] („Hauptvertrag"). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung) sowie dem vorliegenden Vertrag. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 10.5. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 10.1 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 10.2 dargestellt.

§ 5 Schutzmaßnahmen des Auftragnehmers

(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

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 10.3 aufgeführten Maßnahmen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten bestellt hat. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DS-GVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DS-GVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 3 dieses Vertrags durchführen.

(5) Sollten die Daten des Auftraggebers 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 liegen.

(6) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(7) Ein Wechsel in der Person des Ansprechpartners für den Datenschutz oder des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(8) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Insoweit ist der Auftraggeber auch berechtigt, z. B. Auskünfte des Auftragnehmers einzuholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen zu lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich zu prüfen bzw. durch einen sachkundigen Dritten prüfen zu lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber hat insoweit sicherzustellen, dass mögliche Kontrollen nur im erforderlichen Umfang und unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig gestört werden.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 5 Abs. 4 auf Verlangen nach.

§ 8 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 10.4 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis") befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte Betroffener

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

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer allein der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(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 einem Betroffenen eingetreten ist, verantwortlich ist.

(3) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 11 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Schlussbestimmungen

(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.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Oberhausen.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

Anlagen

Anlage 10.1 – Beschreibung der Datenkategorien

Anlage 10.2 – Beschreibung der Betroffenen/Betroffenengruppen

Anlage 10.3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 10.4 – Genehmigte Subunternehmer

Anlage 10.5 – Weisungsberechtigte Personen

Ort, Datum	Unterschrift (Auftraggeber)
Ort, Datum	Unterschrift (Auftragnehmer)

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

Anlage 10.1 – Beschreibung der Datenkategorien

Allgemein speichert der Auftragnehmer zur Auftragsabwicklung, nachhaltigen Betreuung und Kontaktaufnahme mit dem Auftraggeber folgende Daten des Auftraggebers: Firma, Adressen, Ansprechpartner, Telefonnummern, Faxnummern, Mobilfunknummern, E-Mail-Adressen, Ust.-ID, Bankverbindungen, Kundenakte (bestehend aus Auftrags-, Liefer- und Rechnungshistorie, Mahnungen, Support-Tickets und E-Mail-Verlauf), Dokumente, Projekthistorie, Zugangsdaten, Lizenzschlüssel.

Sofern der Auftraggeber die copago Cloud oder Kommunikationsdienste nutzt, werden darüber hinaus folgende Daten gespeichert:

IP-Adressen

Mitarbeiterdaten:

Stammdaten, wie Name, Vorname, Anrede, Anschrift, Telefonnummer, Mobiltelefonnummer, Eintrittsdatum, Geburtsdatum, Mitarbeiterbilder;
Eigenschaften, wie Rollen, Berechtigungen, Kennwörter, erlaubte Rabatte;
Aufzeichnungsdaten, wie Stempelzeiten (Kommen / Gehen), Verkaufshistorie / Bonjournal, Bonstornos, Zeilenstornos, Bildschirmstornos, Mitarbeiter-Kassendifferenzen, Mitteilungen und erhaltene Rabatte, Einkaufshistorie;
Guthaben, wie Prepaid-Guthaben oder Treuepunkte inkl. Historie

Lieferantendaten:

Stammdaten, wie Name, Vorname, Anrede, Firma, Anschriften, Telefonnummern, Mobiltelefonnummern, Geburtsdatum, Lieferantengruppe, lieferbare Artikel;
Preise, wie Einkaufspreise und Kundenverkaufspreise
Aufzeichnungsdaten, wie Einkaufshistorie

Kundendaten:

Grundsätzlich erfolgt der Verkauf an Kunden anonym, es sei denn, der Kunde wurde als Stammkunde registriert. Bei Stammkunden werden folgende Daten gespeichert:
Stammdaten, wie Name, Vorname, Anrede, Firma, Anschriften, Telefonnummern, Mobiltelefonnummern, Geburtsdatum, Kundenbild, Kundengruppe, Eintrittsdatum;
Eigenschaften, wie Sperrkennzeichen und Lieferschein-Berechtigung, Kartennummern, Filial-Zuordnungen, erlaubte Rabatte, Standard-Verkaufsartikel;
Preise, wie Kunden-Verkaufspreise
Aufzeichnungsdaten, wie Verkaufshistorie / Bonjournal, Lieferschein-Einkäufe, Mitteilungen, erhaltene Rabatte;
Guthaben, wie Prepaid-Guthaben oder Treuepunkte inkl. Historie, offene Rechnungen

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

Anlage 10.2 – Beschreibung der Betroffenen/Betroffenengruppen

Erfasst werden Daten von Mitarbeitern, Kunden und Lieferanten.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

Anlage 10.3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Im Folgenden werden die technischen und organisatorisch Maßnahmen der copago AG, gegliedert und differenziert nach den jeweiligen Sicherheitszielen, beschrieben.

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

Zutrittskontrolle
Bei copago sind die folgenden Maßnahmen zur Zutrittskontrolle getroffen, mit denen Unbefugten der physische Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden sowie zu den vertraulichen Akten und Datenträgern verwehrt wird:

- Alle Außentüren zu den Geschäftsräumen von copago sind verschlossen. Zutrittssicherung an allen Zutrittsmöglichkeiten zu den IT-Systemen und Datenverarbeitungsanlagen.
- Elektronisches Zutrittskontrollsystem mittels Transponderzugangssystem
- Sicherheitstüren (Brandschutz).
- Die Reinigung der Geschäftsräume erfolgt innerhalb der Arbeitszeit durch externes Reinigungspersonal.
- Ein zentraler Eingangsbereich mit Empfang ist vorhanden.
- Ein Zutritt von betriebsfremden Personen/Gästen/Besuchern und sonstigen Dritten zu den Geschäftsräumen ist nur in Begleitung einer zutrittsberechtigten Person möglich.
- Besucherüberwachung (Kunden, Wartungspersonal, Handwerker, usw.) in Form von Begleitung durch Beschäftigte in den Geschäftsräumen.
- Die Zutrittsberechtigungen sind im Zutrittsberechtigungssystem hinterlegt. Die Steuerung und deren Entzug erfolgt zentral auf Weisung der Geschäftsführung.
- Dokumentation und Verwaltung der Transponder- und Schlüsselvergabe.

Zugangskontrolle
Bei copago sind die folgenden Sicherheitsmaßnahmen zur Zugangskontrolle getroffen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Alle Datenverarbeitungsanlagen sind zugangsgeschützt.
- Zur Anmeldung/Log-In gegenüber der Datenverarbeitungsanlage muss der Benutzer seiner Benutzerkennung (User-ID) und sein persönliches Passwort eingeben.
- Das Passwort wird sofort gesperrt, falls die Berechtigung erlischt.
- Passwortverfahren mit Intervall und Komplexität (sofern technisch möglich).
- Die Passwort-Policy wird organisatorisch durch Passwortrichtlinie und technisch durch Systemeinstellungen gestaltet.
- Manuelle Zugangssperren für die Arbeitsstationen und Terminals durch manuelle Aktivierung des kennwortgeschützten Bildschirmschoners, durch Sperrung des Systems oder Abmeldung.
- Zusätzlicher System-Log-In für bestimmte Anwendungen.
- Firewall und Netz-Segmentierungen der internen Netzwerke als Abschottung gegen ungewollten Zugang und Zugriffe von außen.
- Viren Scanner.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

- Scannen des ein- bzw. ausgehenden E-Mail- und Web-Verkehrs über verschiedene Schutzsysteme.

Zugriffskontrolle
Bei copago sind die folgenden Maßnahmen zur Zugriffskontrolle getroffen, die zur Benutzung eines Datenverarbeitungssystems berechtigte Personen ausschließlich auf Daten entsprechend ihrer Zugriffsberechtigung zugreifen lassen können, so dass personenbezogene Daten bei der Verarbeitung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

- Zugriff auf Datenverarbeitungssysteme des Auftraggebers im Regelfall über einen Fernzugriffszugang und Authentisierung durch verwendete Passwörter und Protokolle.
- Aufgabenbezogene Berechtigungsprofile durch Reglementierung oder Vergabe durch den Auftraggeber.
- Verwaltung von Berechtigungen; „Prinzip der minimalen Berechtigung". Jeder Beschäftigte erhält nur die Berechtigungen, die für die Erfüllung seiner Tätigkeit minimal erforderlich sind.
- Differenzierte Berechtigungen.
- Vergabe und Entzug von Berechtigungen.
- Protokollierung der Zugriffe.
- Entsorgung von Festplatten/Datenträgern durch zertifizierten Dienstleister.
- Entsorgung von Papier über einen Schredder (nach DIN66399). Alternativ: Vernichtung erfolgt durch ein zertifiziertes Fachunternehmen.

Trennungskontrolle
Bei copago sind die folgenden Maßnahmen zur Trennungskontrolle getroffen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Trennung von Produktiv- und Testumgebungen
- Trennung durch getroffene Zugriffsregelungen sowie Dateiseparierung
- Festlegung von unterschiedlichen Datenbankrechten
- Die Datenbestände der Auftraggeber und deren Projekte werden in den Datenbanken und Mandanten logisch und/oder physisch getrennt, so dass eine Verwechslung oder Vermischung von Datenbeständen oder eine zufällige Löschung ausgeschlossen wird.

Pseudonymisierung
Maßnahmen zur Pseudonymisierung werden nicht eingesetzt, da dies die bei der von copago erbrachten Dienstleistung für den Auftraggeber nicht möglich ist.

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

Weitergabekontrolle
Bei copago sind die folgenden Maßnahmen zur Weitergabekontrolle getroffen, die bei der elektronischen Übertragung oder beim Transport von personenbezogenen Daten oder ihrer Speicherung auf Datenträger eingesetzt werden, um unberechtigte Zugriffe, insbesondere zum Lesen, Kopieren, Verändern oder Entfernen dieser Daten zu verhindern, so dass überprüft und festgestellt

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Physikalischer Versand von Daten im Rahmen des mit dem Auftraggeber vereinbarten Verfahren nur auf Anweisung des Auftraggebers und an autorisierte Personen sowie ggf. verschlüsselt nach Vorgaben des Auftraggebers oder nach dem aktuellen Stand der Technik.
- Protokollierung der Verbindung.
- Gesichertes WLAN.
- Gäste WLAN.
- Datenlöschungen werden nur nach schriftlicher Beauftragung durch den Auftraggeber oder auf der Grundlage der vertraglichen Vereinbarungen datenschutzkonform durchgeführt.
- Löschung von Daten nach Auftragsende wird mit dem Auftraggeber individuell vereinbart, soweit im Rahmen der vertraglichen Vereinbarungen überhaupt personenbezogene Daten vorhanden sind.
- Verschlüsselung der Datenträger bei mobilen Endgeräten.

Eingabekontrolle
Bei copago sind die folgenden Maßnahmen zur Eingabekontrolle getroffen, durch die festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

- Systemseitige Protokollierungen der An- und Abmeldevorgänge.
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Änderungen an Kundendaten erfolgen nur im Rahmen der vertraglichen Vereinbarungen und/oder nach ausdrücklicher, Beauftragung durch den Kunden.
- Differenzierte Zugriffsrechte.

Auftragskontrolle
Bei copago sind die folgenden Maßnahmen zur Auftragskontrolle getroffen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Reinigungs-, Entsorgungs- und Transportpersonal und andere weitere Dienstleister, deren Leistung nicht den konkreten Auftrag als Unterauftragnehmer, sondern indirekt eine Hilfstätigkeit betrifft, werden sorgfältig ausgewählt.
- Zur Gewährleistung des Schutzes und der Sicherheit werden auch bei fremd vergebenen Nebenleistungen angemessene vertragliche Vereinbarungen getroffen.
- Bestimmung von Ansprechpartnern und Projektverantwortlichen für den konkreten Auftrag.
- Bei Auftragsverarbeitung schriftlicher Vertrag gemäß Art. 28 Abs. 3 DS-GVO.
- Keine Beauftragung von Unterauftragnehmern ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers. Abschluss von Verträgen über Auftragsverarbeitung nach Art. 28 Abs. 4 DS-GVO im Falle einer Beauftragung eines Unterauftragnehmers.

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

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

Verfügbarkeitskontrolle
Bei copago sind die folgenden Maßnahmen getroffen, die gewährleisten, dass Daten nicht zufällig verloren gehen oder zerstört werden:

- Um die Verfügbarkeit sicherzustellen, erfolgen intern regelmäßige Datensicherungen.
- Unsere externen Dienstleister sind vertraglich dazu verpflichtet, Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B. durch definierte Backup-Strategien (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne zu sichern.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft.
- Sicherheitsvorfälle werden dokumentiert und ausgewertet.
- Ein Datenschutzbeauftragter wurde bestellt.
- Verpflichtung aller Beschäftigten auf die Einhaltung der datenschutzrechtlichen Anforderungen
- Unterrichtung und Verpflichtung der Beschäftigten über Vertraulichkeits- und Sorgfaltspflichten im Zusammenhang mit der Bearbeitung von Daten und Projekten
- Fremdpersonal ist ebenfalls auf Vertraulichkeit verpflichtet.

5. Weitere Maßnahmen

- Neu eingestellte Beschäftigte werden im Rahmen der Einarbeitung auch zur Einhaltung der Maßnahmen hinsichtlich des Datenschutzes und Informationssicherheit geschult.
- Beschäftigte, die das Unternehmen verlassen (unabhängig von der Art der Beendigung und durch welche Vertragspartei die Beendigung veranlasst wurde), haben im Rahmen des Check-Out-Verfahrens sämtliche empfangene Türschlüssel und Schlüsselkarten abzugeben. Neben der Abgabe der benutzten Hardware werden Benutzerkennungen sowie Zugangs- und Zutrittsberechtigungen sofort gesperrt bzw. dauerhaft gelöscht.
- Die Beschäftigten werden angehalten, nach Abschluss der Arbeiten auf geschlossene Fenster, Sichern aller Türen usw. zu achten.

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

Anlage 10.4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

HP Deutschland GmbH
Schickardstraße 32, 71034 Böblingen

Toshiba Global Commerce Solutions (Germany) GmbH
Carl-Schurz-Straße 7, 41460 Neuss, Deutschland

Microsoft Ireland Ltd.
70 Sir John Rogerson's Quay, Dublin 2, Irland

Google Ireland Ltd.
Gordon House, Barrow Street, Dublin 4, Irland

STRATO AG
Pascalstraße 10, 10587 Berlin, Deutschland

Hetzner Online GmbH
Industriestraße 25, 91710 Gunzenhausen, Deutschland

1blu AG
Stromstraße 1-5, 10555 Berlin, Deutschland

KMZ Kassensystem GmbH
Linsenäcker 15, 72379 Hechingen

KMZ Kassensysteme Nord AG
Papenreye 16, 22453 Hamburg

EMURA GmbH
Albert-Einstein-Straße 26
49076 Osnabrück

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf

Anlage 10.5 – Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers sind

Weisungsempfänger beim Auftragnehmer sind

Dominik Skora
Karl-Heinz Faulhaber

copago AG
Zum Aquarium 6a
46047 Oberhausen
Deutschland

Sitz: Oberhausen
Amtsgericht: Duisburg
HRB 35801

Vorstand:
Dominik Skora
Karl-Heinz Faulhaber
Aufsichtsratsvorsitzender:
Sascha Kaierle

Bankverbindung Sparkasse Krefeld:
IBAN: DE65 3205 0000 0000 3264 47
BIC: SPKRDE33XXXX
Bank: Sparkasse Krefeld

Bankverbindung Commerzbank:
IBAN: DE11 3004 0000 0121 2703 00
BIC: COBADEDDXXX
Bank: Commerzbank Düsseldorf