

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

und

Auftraggeber (Verantwortlicher)

Auftragsverarbeiter

Paul Paasche

Crewlo

Elisabethstraße 20

18057 Rostock

Paul@crewlo.de

im Folgenden: **Auftraggeber**

im Folgenden: **Auftragnehmer**

1. Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 der EU-Datenschutzgrundverordnung (im Folgenden „DSGVO“)

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Textform nach § 126b BGB ausreichend. Die Zustimmung des Auftraggebers zu diesem Vertrag kann durch elektronische Erklärung, insbesondere durch Bestätigung im Rahmen des Onboarding-Prozesses der Software, erfolgen. Zeitpunkt und Umstand der Zustimmung werden vom Auftragnehmer dokumentiert.

Gegenstand und Dauer der Verarbeitung

2.1. Der Auftragnehmer übernimmt folgende Verarbeitungen:

Die Erhebung, Erfassung, Speicherung, Verwendung, Abfrage und Löschung folgender personenbezogener Daten der Beschäftigten des Auftraggebers:

Beschäftigtenstammdaten:

- Vor- und Nachname
- E-Mail-Adresse
- Telefonnummer (freiwillig)
- Anstellungsverhältnis
- Vertragliche Sollstunden (monatliches Stundenlimit)
- Interne Systemrolle (Employee / Shift Manager)
- Firebase UID (technische Nutzerkennung)
- Erstellungsdatum des Nutzeraccounts
- Zeitpunkt der Zustimmung zur Datenschutzerklärung
- Zugehörigkeit zum Mandanten (Tenant-ID)

Arbeitszeit- und Schichtdaten:

- Geplante Schichten (Datum, Startzeit, Endzeit)
- Tatsächlich geleistete und bestätigte Stunden
(Datum, Startzeit, Endzeit)
- Überstundensaldo pro Beschäftigtem

Organisatorische Daten des Auftraggebers:

- Tagesnotizen im Schichtplaner-Kalender
- Interne Rückmeldungen und Feedbacktexte
- Konfigurierte Pausenregeln (Schwellenwert, Pausendauer)
- Eingestellte Öffnungszeiten des Schichtplaner-Kalenders
- Sperrstatus des Kalenders

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden SaaS-Nutzungsvertrag (Crewlo-AGB) in der zum Zeitpunkt des Vertragsschlusses gültigen Fassung

(im Folgenden „Hauptvertrag“).

2.2. Die Verarbeitung beginnt mit dem Zeitpunkt der erstmaligen Nutzung der Software durch den Auftraggeber und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

2. Art und Zweck der Datenverarbeitung

3.1. Der Auftraggeber ist Betreiber eines Unternehmens und nutzt die SaaS-Software „Crewlo“ zur digitalen Schichtplanung und Personalverwaltung seiner Beschäftigten. Der Auftragnehmer ist Anbieter der Software „Crewlo“ und betreibt die zugrundeliegende technische Infrastruktur (Server, Datenbank, Authentifizierungsdienste).

3.2. Die Verarbeitung erfolgt in folgender Art und Weise:

Der Auftragnehmer erhebt, speichert und verarbeitet personenbezogene Daten der Beschäftigten des Auftraggebers ausschließlich im Rahmen der Nutzung der Software „Crewlo“.

Die Daten werden in der Regel vom Auftraggeber (Admin) selbst über die Crewlo-Oberfläche eingegeben und gepflegt. Ausnahme: Bei der erstmaligen Einrichtung des Accounts legt der Auftragnehmer den Administrator-Zugang im Auftrag des Auftraggebers an.

Die Verarbeitung umfasst konkret:

- Speicherung der Daten auf Servern von Hetzner Online GmbH (Deutschland) in einer MySQL-Datenbank
- Authentifizierung der Nutzer über Firebase Authentication (Google Ireland Limited)
- Zugriff auf die Daten ausschließlich durch den Auftraggeber sowie seine berechtigten Beschäftigten entsprechend ihrer Systemrolle
- Zugriff durch den Auftragnehmer (Crewlo) ausschließlich zu technischen Wartungs- und Supportzwecken, soweit dies für den Betrieb der Software erforderlich ist
- Keine Weitergabe der Daten an Dritte außer den in Anlage 2 genannten Subunternehmern

3.3. Die Verarbeitung dient dem Zweck der digitalen Schichtplanung, Arbeitszeitverwaltung und Personalorganisation für den Auftraggeber und erfolgt aufgrund dessen Interesses an einer effizienten, digitalen Verwaltung seiner Beschäftigten sowie der Einhaltung arbeitsrechtlicher Dokumentationspflichten.

3.4. Es werden folgende Kategorien personenbezogener

Daten verarbeitet:

- Allgemeine Personendaten (Vor- und Nachname)

- Kommunikationsdaten (E-Mail-Adresse, Telefonnummer)
- Beschäftigungsdaten (Anstellungsverhältnis, Sollstunden, Systemrolle)
- Arbeitszeitdaten (Schichtzeiten, geleistete Stunden, Überstundensaldo)
- Technische Kennungen (Firebase UID, Tenant-ID, Erstellungsdatum, Zustimmungszeitpunkt Datenschutzerklärung, AGB, und AVV)

3.5. Von der Verarbeitung betroffen sind:

- Beschäftigte des Auftraggebers (Mitarbeiter und Schichtleiter)
- Administratoren des Auftraggebers (z.B. Inhaber, Geschäftsführer, HR-Verantwortliche)

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5. Da der Auftragnehmer als Einzelunternehmer tätig ist, obliegen sämtliche datenschutzrechtlichen Pflichten ausschließlich ihm persönlich.

4.6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.8. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.9. Der Auftragnehmer ist nach aktueller Rechtslage nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Datenschutzrelevante Anfragen sind direkt an paul@crewlo.de zu richten.

4.10. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5. Technische und organisatorische Maßnahmen

5.1. Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen (technische und organisatorische Maßnahmen) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

5.2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen, die das vereinbarte Datenschutzniveau unterschreiten würden, sind zwischen den Parteien zu vereinbaren. Technische Verbesserungen und Upgrades bedürfen keiner gesonderten Vereinbarung.

5.3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6. Der Auftragnehmer stellt sicher, dass der Zugriff auf personenbezogene Daten auch bei Verarbeitung im Homeoffice nur über gesicherte, passwortgeschützte Geräte und verschlüsselte Verbindungen erfolgt.

5.7. Dedizierte digitale Zugänge und Systeme, die für den Auftraggeber genutzt werden, sind durch Zugangsbeschränkungen gesichert. Zugriffe auf das System werden über Server-Logs (Nginx) protokolliert.

5.8. Der Auftraggeber ist berechtigt, die Erfüllung der Pflichten durch den Auftragnehmer im Rahmen der in Ziffer 8.5 geregelten Bedingungen zu kontrollieren. Bei SaaS-Dienstleistungen erfolgt die Kontrolle durch:

- Einsichtnahme in relevante Dokumentationen und Nachweise auf Anfrage
- Bereitstellung von Auskünften durch den Auftragnehmer

6.Regelungen zur Berichtigung, Löschung und Sperrung von Daten

6.1.Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

6.2 Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7. Unterauftragsverhältnisse

7.1. Die Beauftragung von Subunternehmern ist auf Basis der in Anlage 2 aufgeführten Liste zugelassener Subunternehmer gestattet. Der Auftragnehmer ist berechtigt, Subunternehmer hinzuzufügen oder auszutauschen. Über Änderungen informiert der Auftragnehmer den Auftraggeber mindestens 30 Tage vor Inkrafttreten in Textform. Der Auftraggeber kann Änderungen innerhalb von 14 Tagen nach Mitteilung widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Im Falle eines berechtigten Widerspruchs sind die Parteien berechtigt, den Hauptvertrag außerordentlich zu kündigen.

7.2. Bei der Beauftragung neuer Subunternehmer stellt der Auftragnehmer sicher, dass diesen vertraglich mindestens Datenschutzpflichten auferlegt werden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

7.3. Der Auftraggeber kann die Einhaltung der Datenschutzpflichten durch die Subunternehmer über deren öffentlich verfügbare Compliance-Dokumentation nachvollziehen. Bei Google Firebase steht diese unter firebase.google.com/terms/data-processing-terms zur Verfügung, bei Hetzner unter hetzner.com. Eine darüberhinausgehende Kontrolle beim Subunternehmer ist aufgrund der Natur der genutzten Cloud-Dienste nicht möglich. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle ihm vorliegenden Nachweise der Subunternehmer zur Verfügung.

7.4. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

7.5. Eine weitere Subbeauftragung durch den Subunternehmer ist nur zulässig, soweit dieser seinerseits vergleichbare Datenschutzpflichten auferlegt. Bei etablierten Cloud-Anbietern (z.B. Google, Hetzner) gelten deren veröffentlichte Sub-Processor-Listen als Nachweis.

7.6. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.7. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Diese wird dem Auftraggeber auf Anfrage unverzüglich zur Verfügung gestellt.

7.8. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Ziffer 4.10. dieses Vertrages genannten Bedingungen möglich. Im Falle von Firebase Authentication (Google Ireland Limited) erfolgt die Datenübermittlung in die USA auf Grundlage des EU-US Data Privacy Framework (Angemessenheitsbeschluss der EU-Kommission vom 10. Juli 2023) sowie der Google Data Processing Terms.

7.9. Der Auftragnehmer überzeugt sich in angemessenen Abständen davon, dass die eingesetzten Subunternehmer ihre Datenschutzpflichten einhalten. Bei etablierten Cloud-Anbietern gilt deren öffentlich verfügbare Compliance-Dokumentation als ausreichender Nachweis. Diese wird dem Auftraggeber auf Anfrage unverzüglich zur Verfügung gestellt.

7.10. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7.11. Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

7.12. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8. Rechte und Pflichten des Auftraggebers

8.1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

8.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

8.3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

8.4. Der Auftraggeber ist berechtigt, die Einhaltung der Datenschutzvorschriften beim Auftragnehmer durch Einholung von Auskünften, Einsichtnahme in relevante Dokumentationen sowie Anforderung von Nachweisen zu kontrollieren. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen und Nachweise bereitzustellen.

8.5. Kontrollen haben ohne vermeidbare Störungen zu erfolgen. Soweit nicht aus dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung von mindestens 7 Werktagen und nicht häufiger als alle 12 Monate statt.

9. Mitteilungspflichten

9.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 72 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis zu erfolgen. Als Meldeadresse gilt die E-Mail-Adresse des Administrator-Accounts des Auftraggebers, sofern keine abweichende Adresse in Textform benannt wurde. Sie muss mindestens folgende Angaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

9.2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

10. Weisungen

10.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

10.3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10.5. Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Beendigung des Auftrags

11.1. Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Löschung hat so zu erfolgen, dass eine Wiederherstellung der Daten mit vertretbarem Aufwand nicht mehr möglich ist. Bei digitalen Daten erfolgt dies durch unwiderrufliches Löschen aus der Datenbank sowie Deaktivierung und Löschung der zugehörigen Firebase-Accounts.

11.2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

11.3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13. Haftung

13.1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haftet jede Partei für den Bereich, den sie zu verantworten hat. Eine gesamtschuldnerische Haftung besteht nur soweit dies durch Art. 82 DSGVO zwingend vorgeschrieben ist.

13.2. Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Eine Freistellungspflicht besteht nur für Schäden die nachweislich auf einem Verschulden des Auftragnehmers beruhen.

13.3. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

13.4. Die Ziffern 13.2. und 13.3 gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

13.5. Die Haftung des Auftragnehmers ist der Höhe nach auf die Vergütungen begrenzt, die der Auftraggeber in den zwölf Monaten vor Eintritt des schadensbegründenden Ereignisses tatsächlich geleistet hat. Dies gilt nicht bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei vorsätzlich verursachten Schäden.

14. Sonderkündigungsrecht

14.1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

14.2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14.3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

15. Sonstiges

15.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

15.2. Sollten Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

15.3. Für Nebenabreden ist die Textform gemäß § 126b BGB erforderlich..

15.4. Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

15.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

.....

Ort, Datum

Auftraggeber

.....

Ort, Datum

Auftragnehmer

Paul Paasche

Crewlo

Elisabethstraße 20

18057 Rostock

Paul@crewlo.de

Anlage 1

Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Zutrittskontrolle

(Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen)

Da der Auftragnehmer als Einzelunternehmer im Homeoffice tätig ist, erfolgt der Schutz durch:

- Passwortgeschützter Zugang zu allen genutzten Geräten
- Verschlüsselte Verbindung bei Fernzugriff auf Server
- Zugang zum Hetzner-Server ausschließlich über SSH-Schlüssel, kein Passwort-Login

2. Zugangskontrolle

(Schutz vor unbefugter Nutzung von Systemen)

- Authentifizierung aller Nutzer über Firebase Authentication (Google Ireland Limited)
- Rollenbasiertes Zugriffsmodell (Admin, Shift Manager, Employee) – jeder Nutzer sieht nur die Daten die seiner Rolle entsprechen
- Server-Zugang ausschließlich über SSH-Schlüssel
- Alle Verbindungen verschlüsselt über HTTPS/TLS 1.2+

3. Zugriffskontrolle

(Schutz vor unbefugtem Zugriff auf Daten)

- Mandantentrennung: Jeder Kunde (Tenant) sieht ausschließlich seine eigenen Daten
- Datenbankzugriff nur über das Backend (Node.js/Express)
- Kein direkter externer Zugriff auf die MySQL-Datenbank
- Rate Limiting zum Schutz vor unbefugten Zugriffsversuchen

4. Weitergabekontrolle

(Schutz bei Übermittlung und Transport von Daten)

- Alle Datenübertragungen verschlüsselt über HTTPS/TLS 1.2+
- Keine Weitergabe von Daten an Dritte außer den in Anlage 2 genannten Subunternehmern
- Keine unverschlüsselte Übertragung personenbezogener Daten

5. Eingabekontrolle (Nachvollziehbarkeit von Dateneingaben)

- Dateneingaben erfolgen in der Regel durch den Auftraggeber (Admin) über die Crewlo-Oberfläche. Ausnahme: Die erstmalige Einrichtung des Administrator-Accounts erfolgt durch den Auftragnehmer (Crewlo).
- Server-Logs dokumentieren Zugriffe auf das System

- *Erstellungsdatum jedes Nutzeraccounts wird gespeichert*

6. Auftragskontrolle

(Datenverarbeitung nur nach Weisung des Auftraggebers)

- *Daten werden ausschließlich gemäß den Bestimmungen dieses Vertrags verarbeitet*
- *Keine Verarbeitung für eigene Zwecke des Auftragnehmers*
- *Subunternehmer sind vertraglich an Weisungen gebunden*

7. Verfügbarkeitskontrolle

(Schutz vor unbeabsichtigtem Datenverlust)

- *Hosting auf Hetzner Online GmbH (Deutschland), ISO 27001 zertifiziert*
- *Automatische tägliche Backups der MySQL-Datenbank*
- *Wiederherstellung der Daten im Fehlerfall möglich*

8. Trennungsgebot

(Getrennte Verarbeitung von Daten verschiedener Kunden)

- *Strikte Mandantentrennung durch Tenant-ID in der Datenbank – jeder Kunde hat ausschließlich Zugriff auf seine eigenen Daten*
- *Keine Vermischung von Daten verschiedener Kunden*

Anlage 2

Zugelassene Subdienstleister

Der Auftraggeber genehmigt der Einsatz der folgenden Subdienstleister durch den Auftragnehmer:

1. Hetzner Online GmbH

*Anschrift: Industriestr. 25, 91710 Gunzenhausen,
Deutschland*

*Auftragsinhalt: Hosting der Anwendung und Datenbank
(Server, MySQL-Datenbank) auf deutschen Servern*

Verarbeitungsort: Deutschland (EU)

*Datenschutzgrundlage: Auftragsverarbeitungsvertrag
gemäß Art. 28 DSGVO*

Weitere Informationen: [hetzner.com/legal/privacy-policy](https://www.hetzner.com/legal/privacy-policy)

2. Google Ireland Limited (Firebase Authentication)

*Anschrift: Gordon House, Barrow Street,
Dublin 4, Irland*

*Auftragsinhalt: Authentifizierung der Nutzer
(Login, Passwörter, Firebase UID)*

Verarbeitungsort: EU/USA

*Datenschutzgrundlage: EU-US Data Privacy Framework
(Angemessenheitsbeschluss der EU-Kommission vom
10. Juli 2023) sowie Google Data Processing Terms*

Weitere Informationen:

firebase.google.com/terms/data-processing-terms

Anlage 3

Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

1. Weisungserteilung (durch den Auftraggeber)

Die zur Weisungserteilung berechnigte Person auf Seiten des Auftraggebers ist der Administrator-Account, über den die Zustimmung zu diesem Vertrag erteilt wurde.

2. Weisungsentgegennahme (durch den Auftragnehmer)

Name: Paul Paasche

Position: Inhaber / Gründer Crewlo

E-Mail: paul@crewlo.de