Vertrag über Auftragsverarbeitung

im Sinne von Art. 28 Abs. 3 DSGVO

zwischen

der Kunde gemäß Hauptvertrag

nachfolgend „Auftraggeber“

und

DCom Systems KG
Stiller Weg 11
22607 Hamburg

nachfolgend „Auftragnehmer“

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber.

1.2 Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind Anlage 1 zu entnehmen.

1.3 Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung oder nach vorheriger Weisung des Auftraggebers.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls der Auftragnehmer der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis – oder bis zu einer Einräumung sonstiger angemessener Sicherheiten durch den Auftraggeber zur Abwendung von Schäden des Auftragnehmers – ausgesetzt werden.

3.2 Eine von den Weisungen oder ohne Weisungen des Auftraggebers abweichende Verarbeitung ist nur zulässig, wenn der Auftragnehmer nach dem Recht der Europäischen Union oder der

Mitgliedstaaten zur Datenverarbeitung verpflichtet ist. Im Falle einer solchen Verarbeitung, informiert der Auftragnehmer den Auftraggeber unverzüglich über beabsichtigte oder bereits eingeleitete Verarbeitung, es sei denn, dass das betreffende Recht der Europäischen Union oder des Mitgliedstaates eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet; in diesem Fall erfolgt die Mitteilung unverzüglich, sobald die rechtlichen Hindernisse nicht mehr bestehen.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine Weisung in Textform erfolgen konnte. Der Auftragnehmer hat Person, Datum und Uhrzeit der durch den Auftraggeber erteilten Weisung in angemessener Form zu dokumentieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig, im erforderlichen Umfang, zu kontrollieren. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen.

4.2 Die Ergebnisse der Kontrollen und Weisungen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragnehmers

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur zulässig, wenn der Auftragnehmer nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Datenverarbeitung verpflichtet ist. Im Falle einer solchen Verarbeitung, informiert der Auftragnehmer den Auftraggeber unverzüglich über beabsichtigte oder bereits eingeleitete Verarbeitung, es sei denn, dass das betreffende Recht der Europäischen Union oder des Mitgliedstaates eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet; in diesem Fall erfolgt die Mitteilung unverzüglich, sobald die rechtlichen Hindernisse nicht mehr bestehen.

5.2 Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen überprüfen und anpassen.

7. Unterstützungspflichten von Auftragnehmer

Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32-36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragnehmer zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 3 aufgeführt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8.2 Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird der Auftragnehmer dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des/der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des/der Subunternehmer(s) als genehmigt. In dringenden Fällen (z.B. bei kurzfristig benötigten Fehleranalysen oder Mängelbeseitigungen), kann der Auftragnehmer die Anzeige- und Widerspruchsfrist für Subunternehmer angemessen verkürzen. Erfolgt ein fristgerechter Widerspruch, dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und/oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

8.3 Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter (Auftragnehmer) und Unterauftragsverarbeiter (Subunternehmer) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche der Auftragnehmer zur Ausübung von geschäftlichen Tätigkeiten in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen sowie sonstige Maßnahmen, welche die Vertraulichkeit und/oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8.4 Sämtliche Verträge zwischen dem Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmer) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8.5 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

8.6 Dienste, die der Auftraggeber über eigene Konten und Zugangsdaten an Octoserv anbindet

(zum Beispiel Anbieter von KI-Modellen, E-Mail-Versanddienste, Brief- und Druckdienste, Werbeplattformen, Telefonie- und Messengerdienste), sind keine Unterauftragsverarbeiter des Auftragnehmers. Der Auftraggeber schließt die Verträge mit diesen Anbietern selbst, einschließlich etwa erforderlicher Vereinbarungen zur Auftragsverarbeitung, und entscheidet selbst, welche Daten an sie übermittelt werden. Der Auftragnehmer stellt lediglich die technische Verbindung bereit und übermittelt Daten nur auf Veranlassung des Auftraggebers. Welche Funktion welche Daten an welche Art von Dienst übermittelt, ergibt sich aus Anlage 4.

9. Mitteilungspflichten des Auftragnehmers

9.1 Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer beim Auftragnehmer angestellten Person, einem Subunternehmer oder einer sonstigen Person, die der Auftragnehmer zur Erfüllung vertraglicher Pflichten eingesetzt hat, begangen wurde.

9.2 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten und das weitere Vorgehen mit ihm abstimmen.

9.3 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von denen auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern für den Auftragnehmer keine rechtliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich, Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist der Sitz des Auftragnehmers Gerichtsstand für alle Streitigkeiten aus diesem Vertrag; ausschließliche Gerichtsstände bleiben hiervon unberührt.

12.3 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während

der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.4 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.5 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Abschluss in elektronischer Form

Dieser Vertrag wird in elektronischer Form abgeschlossen (Art. 28 Abs. 9 DSGVO). Er kommt zustande, indem der Auftraggeber ihn bestätigt oder in seinen Hauptvertrag einbezieht. Eine handschriftliche Unterschrift ist nicht vorgesehen. Wurde der Vertrag bestätigt, nennt der Vermerk „Elektronisch abgeschlossen“ am Ende des Vertrags die bestätigende Person, den Zeitpunkt und die Fassung.

Anlage 1 - Auftragsdetails

Leistung	Datenarten	Betroffene Personenkategorien
Webhosting	• IP-Adressen von Webseitenbesuchern • Eingaben in Kontaktformulare • Analysen zum Nutzerverhalten • Kundendaten • Kontakt- und Firmendaten im CRM (Name, Anschrift, Telefon, E-Mail, Notizen, Verlauf), E-Mails und Anhänge, Termine, Angebote, Rechnungen und Verträge, Dokumente, Chat- und Telefonieverläufe, Zugangsdaten der Benutzer	• Webseitenbesucher des Auftraggebers • Kunden des Auftraggebers • Interessenten des Auftraggebers, Ansprechpartner von Geschäftspartnern, Beschäftigte und Benutzer des Auftraggebers
Bereitstellung, Betrieb, Wartung, Datensicherung und Support der Software Octoserv (auf der Plattform von DCom oder auf einem Server, den DCom für den Auftraggeber betreibt)	Alle Daten, die der Auftraggeber in Octoserv speichert oder verarbeiten lässt: Kontakt- und Firmendaten, Kommunikationsdaten (E-Mails, Chats, Anrufprotokolle), Formulareingaben, Termine, Angebote, Rechnungen, Verträge, Dokumente, Einwilligungen, Nutzungs- und Protokolldaten, Benutzerkonten. Beim Support Einsicht nur im erforderlichen Umfang.	Kunden, Interessenten und Geschäftspartner des Auftraggebers und deren Ansprechpartner, Besucher der Websites und Formulare des Auftraggebers, Beschäftigte und Benutzer des Auftraggebers

Anlage 1 (Fortsetzung) - Datenarten und Betroffene je freigeschaltetem Modul

Die folgende Aufstellung wurde aus den Modulen erzeugt, die für diese Installation freigeschaltet sind.

Modul	Datenarten	Betroffene Personenkategorien
Octoserv (Grundfunktionen)	• Kontakt- und Firmendaten (Name, Anschrift, Telefon, E-Mail, Notizen, Verlauf) • E-Mails und Anhänge • Termine, Aufgaben und Dokumente • Formulareingaben und Einwilligungen • Nutzungs- und Protokolldaten (Journal) • Benutzerkonten und Zugangsdaten der Benutzer	• Kunden, Interessenten und Geschäftspartner des Auftraggebers und deren Ansprechpartner • Besucher der Websites und Formulare des Auftraggebers • Beschäftigte und Benutzer des Auftraggebers
Rechnungen	• Rechnungsdaten (Empfänger, Positionen, Beträge, Zahlungen, Mahnungen) • Rechnungs-PDF	• Kunden des Auftraggebers und deren Ansprechpartner
Angebote	• Angebotsdaten (Empfänger, Positionen, Preise, Texte) • Angebots-PDF • Aufrufe der Angebotsseite	• Interessenten und Kunden des Auftraggebers und deren Ansprechpartner
Serienbriefe	• Anschrift und Inhalt der Briefe • Versandstatus beim Briefdienst	• Empfänger der Briefe
Telefonie	• Rufnummern • Anrufprotokolle (Zeit, Dauer, Richtung) • Aufzeichnungen und Notizen zu Anrufen	• Anrufer und Angerufene • Beschäftigte des Auftraggebers
WhatsApp	• Rufnummern • Nachrichten und Medien der Konversationen	• Kunden und Interessenten des Auftraggebers
Livechat	• Chat-Nachrichten • Angegebene Kontaktdaten • Seitenverlauf der Chat-Sitzung	• Besucher der Websites des Auftraggebers • Beschäftigte des Auftraggebers

Modul	Datenarten	Betroffene Personenkategorien
Support	• Support-Anfragen, Nachrichten und Anhänge • Aufnahmen (Bildschirm, Kamera, Sprache) • Zeitbuchungen	• Kunden des Auftraggebers und deren Ansprechpartner • Beschäftigte des Auftraggebers
RagChat	• Fragen und Antworten im Chat der Website • Bewertungen der Antworten	• Besucher der Websites des Auftraggebers
Tracking (OctoLytics)	• Seitenaufrufe und Klicks • Technische Angaben zum Besuch (Browser, Gerät, Adresse des Besuchers, Herkunft) • Conversion-Ereignisse	• Besucher der Websites des Auftraggebers
Landingpages	• Eingaben in Formulare der Landingpages • Seitenaufrufe	• Besucher der Landingpages des Auftraggebers
SEO	• Domains, Seiteninhalte und Messwerte zur Sichtbarkeit der Websites des Auftraggebers	• Betreiber und Ansprechpartner der Websites des Auftraggebers
Ads	• Kennzahlen der Werbekonten • Konversionsereignisse, die an Werbeplattformen übergeben werden	• Besucher und Interessenten des Auftraggebers
Leadgenerierung	• Firmen- und Kontaktangaben von Interessenten aus öffentlichen Quellen • Bewertungen der Interessenten	• Ansprechpartner von Unternehmen, die der Auftraggeber als Interessenten sucht
Projekte	• Projekte, Aufgaben, Kommentare und Dateien • Zeiterfassung	• Kunden des Auftraggebers und deren Ansprechpartner • Beschäftigte des Auftraggebers
Workflows	• Vorgänge mit Formulareingaben, Zuständigkeiten, Freigaben und Dateien	• Beteiligte der Vorgänge (Kunden, Beschäftigte des Auftraggebers)
Videoräume	• Namen und Zugangsschlüssel der Teilnehmer • Kursfortschritt	• Teilnehmer der Videoräume
Connector	• Daten, die mit einem angebundenen Fremdsystem abgeglichen werden (Kontakte, Firmen und Vorgänge nach der eingestellten Zuordnung)	• Personen, deren Daten im Fremdsystem und in Octoserv geführt werden
Ranking	• Bewertung von Kontakten aus ihrem Verhalten (Öffnungen, Klicks, Seitenbesuche, Antworten)	• Interessenten und Kunden des Auftraggebers
Dubletten	• Kontakt- und Firmendaten zum Abgleich auf Dubletten	• Kontakte des Auftraggebers
Opt-in-Status	• Einwilligungen und Abmeldungen je Adresse und Thema • Rückläufer	• Empfänger von E-Mails des Auftraggebers
Änderungsprotokoll	• Protokoll der Änderungen (Benutzer, Zeitpunkt, Werte)	• Benutzer des Auftraggebers und die Personen, deren Daten geändert wurden
Finanzen	• Belege, Buchungen, Bankumsätze • Angaben zu Kunden und Lieferanten	• Kunden und Lieferanten des Auftraggebers und deren Ansprechpartner
OctoPages	• Kontaktangaben, Briefing, Inhalte und Freigaben zur Erstellung von Webseiten	• Kunden des Auftraggebers und deren Ansprechpartner
TK-Aufnahme	• Angaben zur Telefonanlage und zu den Anschlüssen eines Kunden • Ansprechpartner	• Kunden des Auftraggebers und deren Beschäftigte

Anlage 2 - Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Sicherung der Arbeitsstätte des Auftragsverarbeiters (Zutrittskontrolle)

Die Arbeitsstätte des Auftragsverarbeiters wird in folgender Weise gegen Einbruch und sonstige unbefugte Zutritte gesichert:

Die Server mit den Daten des Auftraggebers stehen nicht in den Büroräumen des Auftragnehmers, sondern in Rechenzentren der Hetzner Online GmbH (Deutschland/Finnland) mit deren Zutrittskontrolle (Zertifizierung nach ISO/IEC 27001). Die Büroräume des Auftragnehmers sind abschließbar (Türschlösser). Die Daten des Auftraggebers werden ausschließlich in Octoserv verarbeitet und nicht auf Arbeitsgeräten abgelegt. Auf Arbeitsrechner und Mobiltelefon gelangen nur E-Mails; beide Geräte sind durch Festplatten- bzw. Geräteverschlüsselung mit Sperrcode geschützt. Geschäftliche Kommunikation über Messenger läuft nicht über private Geräte, sondern über Octoserv.

2. Sicherung der IT-Systeme des Auftragsverarbeiters (Zugangskontrolle)

Die IT-Systeme des Auftragsverarbeiters werden in folgender Weise gegen unbefugte Zugriffe (z.B. Hackerangriffe) gesichert:

- Passwortvergabe
- Erstellen von Benutzerprofilen in den IT-Systemen
- Login in die IT-Systeme mit individuellem Benutzernamen und Passwort
- Zugriffsregeln für Benutzer / Benutzergruppen in den IT-Systemen (Berechtigungskonzept)
- Verwaltung der Berechtigungen durch Systemadministratoren
- Anzahl der Systemadministratoren ist auf das „Notwendigste“ reduziert
- Einsatz von Anti-Viren-Software
- Einsatz von Software-Firewall
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung der Datensicherungssysteme

Server-Zugang nur per SSH-Schlüssel, Anmeldung mit Passwort abgeschaltet; Firewall mit Freigabeliste für den Verwaltungszugang; Sperre wiederholter Fehlanmeldungen (fail2ban); Virenprüfung eingehender E-Mails; Rollen und Rechte je Benutzer in Octoserv, Mandantentrennung auf Datenbankebene; zweiter Anmeldefaktor für Benutzer verfügbar.

3. Protokollierung von Datenverarbeitungsprozessen (Eingabekontrolle)

Folgende Maßnahmen stellen sicher, dass der Auftragsverarbeiter jederzeit erkennen kann, welche Datenverarbeitungsprozesse in seinen Datenverarbeitungssystemen stattgefunden haben (z.B. Eingabe, Veränderung, Sperrung oder Löschung):

- Protokollierung von Zugriffen auf die IT-Systeme des Auftragsverarbeiter (Log-Protokolle)
- Protokollierung von Eingaben, Änderungen und Löschungen (Log-Protokolle)
- Protokollierung der Aktionen einzelner Nutzer

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

Löschung von Daten

Folgende Maßnahmen stellen sicher, dass personenbezogene Daten fristgerecht gelöscht werden:

- Löschkonzept mit Fristen je Datenart (Anlage 5)
- Automatische tägliche Löschung abgelaufener Daten durch die Software, jeder Lauf im Journal protokolliert
- Sperrung statt Löschung bei gesetzlichen Aufbewahrungspflichten und automatische Löschung nach Fristende
- Ausgemusterte Server-Datenträger werden vom Rechenzentrum (Hetzner) nach dessen zertifiziertem Verfahren vernichtet

4. Datenschutz bei den Subunternehmern des Auftragsverarbeiters

Folgende Maßnahmen stellen sicher, dass sich die vom Auftragsverarbeiter ausgewählten Subunternehmer datenschutzkonform verhalten:

- Auswahl der Subunternehmer unter Sorgfaltsgesichtspunkten (insb. hinsichtlich Datensicherheit)
- Abschluss von DSGVO-konformen Auftragsverarbeitungsverträgen mit dem Subunternehmer

5. Sicherung von Daten bei Transport und Übermittlung (Weitergabekontrolle)

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) vor unbefugten Dritten geschützt werden:

- Verschlüsselung des E-Mail-Verkehrs
- Verschlüsselung der sonstigen Kommunikationswege

6. Datensicherung und Backups (Verfügbarkeit und Wiederherstellbarkeit)

Folgende Maßnahmen stellen sicher, dass die vertragsgegenständlichen Daten jederzeit verfügbar sind:

- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort

Tägliche Sicherung auf dem Server, zusätzlich tägliche verschlüsselte Sicherung außer Haus (Hetzner Storage Box) mit 7 Tages-, 4 Wochen- und 6 Monatsständen; gespiegelte Festplatten (RAID 1); Serverräume, Stromversorgung, Klimatisierung und Brandschutz durch das Rechenzentrum.

7. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

8. Gemessene Angaben zur Installation

Die folgenden Angaben wurden von der Software an der laufenden Installation gemessen. Jede Angabe nennt ihre Quelle.

Angabe	Wert	Quelle
Version der Software	0.1.0	config app.version

Angabe	Wert	Quelle
Datenbank	PostgreSQL 17.11	SHOW server_version
Mandantentrennung auf Datenbankebene (Tabellen mit Zeilenschutz / Tabellen mit Mandantenspalte)	471 / 471	pg_class.relrowsecurity, tables with tenant_id
Verfahren zur Speicherung der Passwörter	bcrypt	config hashing.driver
Verschlüsselung der gespeicherten Zugangsdaten und Schlüssel	XChaCha20-Poly1305	App\Core\Data\SecretData
Zugriff nur über HTTPS	ja	config app.url
Dauer einer Sitzung ohne Aktivität in Minuten	120	config session.lifetime
Aktive Benutzer	1	table tenant_memberships
Aktive Benutzer mit zweitem Anmeldefaktor	0	tables users, passkeys
Das Journal der Änderungen kann von der Anwendung geändert werden	nein	has_table_privilege(events)
Das Journal der Änderungen kann von der Anwendung gelöscht werden	nein	has_table_privilege(events)
Aufbewahrung der Mandantensicherungen in Tagen	7	config backup.keep_days
Aufbewahrung von Rechnungen in Jahren	10	config retention.invoice_years
Aufbewahrung versendeter Angebote in Jahren	6	config retention.business_letter_years
Aufbewahrung einzelner Verhaltensereignisse in Tagen	395	config retention.registry
Aufbewahrung des Protokolls des Cookie-Banners in Tagen	1095	config retention.consent_log_days
Freigeschaltete Module	ads, connector, doublets, dpa, finance, gobd, handbook, invoice, landingpage, leadgen, letters, licenses, livechat, logger, octolytics, octopages, optin_status, postcode_class, projects, proposal, ragchat, ranking, security_report, seo, support, telephony, tk_survey, video, whatsapp, workflows	table tenant_modules
Zeitpunkt der Messung	2026-11-01T15:19:39+00:00	clock of the server

Anlage 3 - Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Name und Anschrift	Leistung	Land der Leistungserbringung
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Rechenzentrum und Server (Hosting der Octoserv-Installation und der Datenbank) sowie Speicherplatz für die verschlüsselte Sicherung außer Haus	Deutschland und Finnland (EU)

Anlage 4 - Datenflüsse je Funktion

Siehe Tabelle „Datenflüsse je Funktion“ in der Octoserv-Hilfe „KI in Octoserv“ (Stand bei Vertragsschluss beifügen).

Anlage 5 - Löschkonzept

1. Zweck und Geltung

Das Konzept regelt, wann personenbezogene Daten in Octoserv und in den Sicherungen gelöscht werden. Es gilt für alle Installationen, die DCom betreibt (Plattform octo.dcom.systems und saas.octoserv.com sowie Server, die DCom für einzelne Kunden betreibt). Verantwortlicher für die Daten ist der Kunde; DCom löscht als Auftragsverarbeiter nach seiner Weisung und nach diesem Konzept.

2. Grundsätze

1. Gelöscht wird, sobald der Zweck entfällt und keine gesetzliche Aufbewahrungspflicht besteht (Art. 5 Abs. 1 lit. e, Art. 17 DSGVO).
2. Unterliegt ein Datensatz einer Aufbewahrungspflicht, wird er bei einem Löschwunsch nicht gelöscht, sondern gesperrt (Art. 18 DSGVO) und nach Fristende automatisch gelöscht.
3. Löschfristen laufen über tägliche Aufträge auf dem Server, nicht von Hand. Jeder Lauf steht im Journal.
4. Aufbewahrungsfristen nach HGB und AO beginnen mit dem Ende des Kalenderjahres, in dem der Datensatz entstanden ist (Beispiel: Rechnung vom 14.03.2026, 10 Jahre, gesperrt bis 31.12.2036, gelöscht ab 01.01.2037).

3. Löschfristen je Datenart

Datenart	Frist	Wie gelöscht	Quelle im Code
Kontakte, Firmen, Notizen, Aufgaben, Termine, Dokumente, Kundenmails	solange der Kunde sie braucht; Löschung durch den Kunden oder auf Antrag der betroffenen Person	Datenschutzanfrage in Octoserv (Auskunft, Löschung); gesetzlich aufzubewahrende Teile werden gesperrt	octo:privacy-requests, F53a
Rechnungen, Zahlungen, Mahnungen mit PDF	10 Jahre	gesperrt, danach automatisch gelöscht	config/retention.php invoice_years, Job octo:retention-expire
Versendete Angebote mit PDF (Handelsbriefe)	6 Jahre	gesperrt, danach automatisch gelöscht	business_letter_years, octo:retention-expire
Verfahrensdokumentation (GoBD) mit Fassungen und Belegen	10 Jahre	aufbewahrt, keine Löschung durch die Anwendung	procedure_documentation_years
Verhaltensdaten (Öffnungen, Klicks, Seitenaufrufe, Anmeldungen) als Einzelereignis	13 Monate (395 Tage); Summen bleiben	täglich gelöscht	behavior_events, octo:behavior-retention
Protokoll des Cookie-Banners	3 Jahre (1.095 Tage), vom Kunden kürzbar auf 30 Tage bis 10 Jahre	täglich gelöscht	consent_log_days, octo:consent-log-prune

Datenart	Frist	Wie gelöscht	Quelle im Code
Versandprotokoll der E-Mails	2 Jahre (730 Tage), vom Kunden einstellbar 30 Tage bis 10 Jahre	täglich gelöscht	MailData::LOG_RETENTION_*
Anmeldeversuche und abgelaufene Sperren	7 Tage, vom Kunden einstellbar 2 bis 365 Tage	täglich gelöscht	octo:sign-in-log-prune
Zustellmeldungen eingehender Webhooks	30 Tage	täglich gelöscht	InboundDeliveryData::RETENTION_DAYS
Nicht abgeschlossene mehrseitige Formulare	14 Tage	täglich gelöscht	octo:form-drafts-purge
Befristete Feldwerte (z. B. Einwilligung bis Datum)	mit Ablauf des Datums geschwärzt oder geleert	täglich	octo:field-expiry
Unbestätigte Datenschutzanfragen, abgelaufene Auskunftspakete	mit Ablauf der Bestätigungsfrist bzw. des Download-Links	stündlich	octo:privacy-requests
Exporte des Kunden	7 Tage	täglich gelöscht	ExportData::KEEP_DAYS
Mandantensicherungen in Octoserv (Einstellungen → Werkzeuge → Sicherung)	7 Tage	täglich gelöscht	config/backup.php keep_days, octo:backups-expire
Server-Sicherung auf srv0	3 Tage	rollierend überschrieben	/usr/local/bin/server-backup.sh (KEEP_DAYS=3)
Verschlüsselte Sicherung außer Haus (Hetzner Storage Box)	7 Tages-, 4 Wochen-, 6 Monatsstände, also höchstens rund 6 Monate	borg prune bei jedem Lauf	/usr/local/bin/borg-backup.sh

4. Löschung bei Vertragsende

1. Der Kunde kann seine Daten bis zum Ende der Exportfrist nach § 20 AGB herunterladen; die Frist beträgt 30 Tage nach Vertragsende.
2. Danach löscht DCom die Installation bzw. den Mandanten mit allen Daten. Daten mit Aufbewahrungspflicht stellt DCom vorher zum Export bereit; die Aufbewahrung liegt dann beim Kunden.
3. In den Sicherungen verschwinden die Daten mit deren regulärem Ablauf (spätestens nach rund 6 Monaten). Eine Wiederherstellung aus einer Sicherung findet nach Vertragsende nicht mehr statt.
4. DCom bestätigt die Löschung auf Wunsch in Textform.

5. Datenträger

DCom betreibt keine eigenen Server-Datenträger; die Server und Speicher stehen bei Hetzner. Ausgemusterte Datenträger vernichtet Hetzner nach seinem eigenen Verfahren (Zertifizierung nach ISO/IEC 27001). Kundendaten liegen nur in Octoserv. Auf Mac und Telefon von DCom gelangen nur E-Mails; der Mac ist mit FileVault verschlüsselt (geprüft am 31.10.2026), das Telefon mit Sperrcode. Geschäftliche Messenger-Kommunikation läuft über Octoserv, nicht über private Geräte.

6. Zuständigkeit und Überprüfung

- Verantwortlich für dieses Konzept bei DCom: Alvaro Moreno.
- Überprüfung alle 12 Monate und bei jeder neuen Datenart in Octoserv. Neue Funktionen mit personenbezogenen Daten bekommen ihre Frist im Code (config/retention.php oder eigener Job) und eine Zeile in Tabelle 3.