Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

FIRMA GmbH
Straße Hausnummer, PLZ Ort
Vert. d. d. Geschäftsführer Vorname Nachname

- Im Folgenden „Auftraggeber“ genannt -

und

cebra GmbH – new technologies
Sankt-Martin-Str. 9, 84539 Ampfing
Vert. d. d. Geschäftsführer Helmut Brandlmeier und Christian Sigl

- Im Folgenden „Auftragnehmer“ genannt -

- Gemeinsam „Parteien“ genannt.

Präambel

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte der cebra GmbH oder durch den Auftragnehmer beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand der Verarbeitung

a. Der Auftragnehmer verarbeitet im Rahmen der vereinbarten IT-Dienstleistungen personenbezogene Daten im Auftrag des Auftraggebers, soweit dies zur Erbringung der jeweiligen Leistungen erforderlich ist.
b. Gegenstand, Art, Zweck und Umfang der Verarbeitung ergeben sich aus dieser Vereinbarung, Anlage I sowie den jeweils zwischen den Parteien vereinbarten Leistungen.
c. Die Verarbeitung kann insbesondere durch Administration, Wartung, Fernwartung, Fehleranalyse, Störungsbehebung, Datensicherung oder sonstigen technischen Zugriff auf Systeme des Auftraggebers erfolgen.
d. Bei Widersprüchen zwischen dieser Vereinbarung und anderen vertraglichen Regelungen zur Auftragsverarbeitung geht diese Vereinbarung hinsichtlich der Auftragsverarbeitung vor.

§ 2 Fernwartung und administrativer Zugriff

Der Auftraggeber gestattet dem Auftragnehmer zur Erbringung der vereinbarten Leistungen den Zugriff auf seine IT-Systeme über:

☒ Fernwartungssoftware
☒ Remotedesktopverbindung
☒ Dauerhaften Fernwartungszugang
☒ Temporären Fernwartungszugang

Der temporäre Fernwartungszugang wird für den jeweils erforderlichen Zeitraum oder für den konkret beauftragten Vorgang eingerichtet und nach Abschluss der Arbeiten deaktiviert oder gelöscht. Eine vorherige Freigabe des Auftraggebers ist erforderlich, soweit dies im Einzelfall vereinbart oder technisch vorgesehen ist.
Bei einem dauerhaften Fernwartungszugang ist keine vorherige Freigabe des Auftraggebers für jeden einzelnen Zugriff erforderlich.
Die Gestattung des Fernzugriffs gilt als dokumentierte Weisung für diejenigen Zugriffe und Verarbeitungsvorgänge, die zur Erbringung der jeweils beauftragten Leistungen erforderlich sind.
Der Auftragnehmer darf den Fernzugriff ausschließlich für die vereinbarten Leistungen und innerhalb des Weisungsrahmens des Auftraggebers nutzen.

§ 3 Dauer der Verarbeitung

Diese Vereinbarung gilt für die Dauer der vertraglichen Leistungen, bei denen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

Sie endet mit Beendigung der entsprechenden Verarbeitungsleistungen. Verpflichtungen, die ihrer Natur nach über die Vertragsbeendigung hinaus gelten, insbesondere Vertraulichkeits-, Lösch- und Nachweispflichten, bleiben hiervon unberührt.

§ 4 Art der personenbezogenen Daten und Kategorien betroffener Personen

a. Die regelmäßig verarbeiteten Datenarten und Kategorien betroffener Personen ergeben sich aus Anlage I.
b. Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sind grundsätzlich nicht Gegenstand einer gezielten Verarbeitung durch den Auftragnehmer. Ein technisch bedingter oder zufälliger Zugriff im Rahmen der vereinbarten IT-Dienstleistungen kann jedoch nicht ausgeschlossen werden.
c. Gleiches gilt für personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO, soweit sich solche Daten auf den vom Auftragnehmer betreuten Systemen befinden.

§ 5 Pflichten des Auftragnehmers

a. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung, der vereinbarten Leistungen und der dokumentierten Weisungen des Auftraggebers, soweit keine gesetzliche Verpflichtung zu einer abweichenden Verarbeitung besteht.
b. Der Auftragnehmer stellt sicher, dass Personen mit Zugriff auf personenbezogene Daten zur Vertraulichkeit verpflichtet sind oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen.
c. Der Auftragnehmer trifft angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die Maßnahmen ergeben sich aus Anlage II und dürfen entsprechend der technischen Entwicklung angepasst werden, sofern das angemessene Schutzniveau nicht unterschritten wird.
d. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im gesetzlich erforderlichen Umfang bei Betroffenenrechten sowie bei den Pflichten gemäß Art. 32 bis 36 DSGVO.
e. Der Auftragnehmer informiert den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, soweit Daten des Auftraggebers betroffen sind.
f. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er eine Weisung für datenschutzrechtlich unzulässig hält. Die Durchführung der betroffenen Weisung darf bis zur Klärung ausgesetzt werden.
g. Ansprechpartner für Datenschutzfragen beim Auftragnehmer ist:
   cebra GmbH – new technologies
   Sankt-Martin-Straße 9
   84539 Ampfing
   E-Mail: datenschutz@cebra.it

§ 6 Zweckbindung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich soweit dies zur Erbringung der vereinbarten Leistungen, insbesondere zur Administration, Wartung, Fernwartung,

Fehleranalyse, Störungsbehebung, Datensicherung und Gewährleistung der IT-Sicherheit erforderlich ist.

Eine Verarbeitung personenbezogener Daten des Auftraggebers zu davon unabhängigen eigenen Zwecken des Auftragnehmers erfolgt nicht.

§ 7 Löschung und Rückgabe

a. Nach Beendigung der jeweiligen Verarbeitungsleistungen gibt der Auftragnehmer die in seinem Besitz befindlichen personenbezogenen Daten nach Wahl des Auftraggebers zurück oder löscht diese, soweit keine gesetzliche Verpflichtung zur weiteren Speicherung besteht.
b. Vorübergehend für Support-, Wartungs-, Migrations- oder Fehleranalysezwecke auf Systeme des Auftragnehmers übertragene Daten werden gelöscht, sobald sie für den jeweiligen Zweck nicht mehr benötigt werden.
c. Soweit Daten in ordnungsgemäß erstellten Sicherungskopien enthalten sind und eine selektive Löschung technisch nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, werden diese bis zum Ablauf des regulären Sicherungs- und Aufbewahrungszyklus gegen produktive Nutzung gesperrt und anschließend gelöscht oder überschrieben.
d. Besondere Vorgaben des Auftraggebers hinsichtlich Datenexport, Datenformat, Datenträgern oder zusätzlicher Löschmaßnahmen, die über die reguläre Leistungserbringung hinausgehen, können nach den vereinbarten Vergütungssätzen abgerechnet werden.
e. Auf Verlangen bestätigt der Auftragnehmer die durchgeführte Löschung in geeigneter Form.

§ 8 Pflichten des Auftraggebers

a. Der Auftraggeber ist für die Rechtmäßigkeit der Erhebung und Verarbeitung der personenbezogenen Daten sowie für die Wahrung der Rechte betroffener Personen verantwortlich.
b. Der Auftraggeber erteilt dem Auftragnehmer die zur Leistungserbringung erforderlichen Weisungen und stellt die hierfür erforderlichen Informationen bereit.
c. Der Auftraggeber informiert den Auftragnehmer unverzüglich über ihm bekannt gewordene Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Auftragsverarbeitung.
d. Der Auftraggeber hält die gegenüber dem Auftragnehmer benannten Ansprechpartner und Kontaktmöglichkeiten aktuell.
e. Eine allgemeine oder fortlaufende rechtliche Prüfung der vom Auftraggeber bestimmten Verarbeitungszwecke oder der vom Auftraggeber bereitgestellten Daten durch den Auftragnehmer ist nicht geschuldet. Die Hinweispflicht des Auftragnehmers bei erkennbar rechtswidrigen Weisungen bleibt unberührt.

§ 9 Weisungen

a. Weisungen können schriftlich, per E-Mail, über das Ticketsystem oder über andere zwischen den Parteien verwendete elektronische Kommunikationswege erteilt werden.
b. Weisungen von Mitarbeitern oder sonstigen Ansprechpartnern des Auftraggebers darf der Auftragnehmer als autorisiert behandeln, soweit für den Auftragnehmer keine begründeten Zweifel an deren Berechtigung bestehen.
c. Mündliche Weisungen sind anschließend in geeigneter Form zu dokumentieren.

d. Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, gelten als Anforderung einer zusätzlichen Leistung und können nach den vereinbarten Vergütungssätzen abgerechnet werden. Der Auftragnehmer ist nicht verpflichtet, solche zusätzlichen Leistungen vor einer entsprechenden Beauftragung auszuführen.
e. Hält der Auftragnehmer eine Weisung für datenschutzrechtlich unzulässig, darf er deren Durchführung bis zur Klärung aussetzen. Besteht der Auftraggeber trotz eines entsprechenden Hinweises auf einer rechtswidrigen Weisung, bleiben weitergehende gesetzliche und vertragliche Rechte des Auftragnehmers einschließlich einer Beendigung der betroffenen Leistung aus wichtigem Grund unberührt.
f. Eine Übermittlung personenbezogener Daten in ein Drittland erfolgt nur aufgrund einer dokumentierten Weisung des Auftraggebers oder im Rahmen ausdrücklich vereinbarter Leistungen und nur unter Einhaltung der Art. 44 ff. DSGVO.

§ 10 Vertraulichkeit

Der Auftragnehmer gewährleistet, dass Personen, die Zugriff auf personenbezogene Daten des Auftraggebers erhalten können, zur Vertraulichkeit verpflichtet sind oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen.

Die Verpflichtung besteht auch nach Beendigung der jeweiligen Tätigkeit fort.

§ 11 Weitere Auftragsverarbeiter

a. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung zur Inanspruchnahme weiterer Auftragsverarbeiter gemäß Art. 28 Abs. 2 DSGVO.
b. Die zum Zeitpunkt des Vertragsschlusses vorgesehenen weiteren Auftragsverarbeiter ergeben sich aus Anlage III. Reine Lieferanten, Hersteller, Distributoren oder Lizenzgeber, die keine personenbezogenen Daten des Auftraggebers im Auftrag des Auftragnehmers verarbeiten, sind keine weiteren Auftragsverarbeiter im Sinne dieser Vereinbarung.
c. Der Auftragnehmer informiert den Auftraggeber vor der Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters in Textform, insbesondere per E-Mail an die zuletzt vom Auftraggeber mitgeteilte Kontaktadresse. Die Information enthält mindestens die Identität des weiteren Auftragsverarbeiters und die Art der vorgesehenen Verarbeitung.
d. Der Auftraggeber kann innerhalb von 14 Kalendertagen nach Zugang der Information aus konkreten und berechtigten datenschutzrechtlichen Gründen widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, darf der weitere Auftragsverarbeiter eingesetzt werden.
e. Im Falle eines berechtigten Widerspruchs prüfen die Parteien eine zumutbare Alternative. Ist die Erbringung der betroffenen Leistung ohne den weiteren Auftragsverarbeiter nicht oder nur mit unverhältnismäßigem Aufwand möglich, ist der Auftragnehmer berechtigt, die betroffene Leistung mit einer Frist von 30 Tagen zu kündigen. Eine vom Auftraggeber gewünschte alternative technische Lösung kann als zusätzliche Leistung vereinbart und vergütet werden.
f. Der Auftragnehmer verpflichtet weitere Auftragsverarbeiter gemäß Art. 28 Abs. 4 DSGVO zu den erforderlichen Datenschutzpflichten und bleibt im gesetzlich vorgesehenen Umfang für deren Einhaltung verantwortlich.

g. Der Auftragnehmer hält die für Art. 28 DSGVO erforderlichen Informationen über die eingesetzten weiteren Auftragsverarbeiter und die Verarbeitungskette aktuell und stellt sie dem Auftraggeber auf Anfrage in elektronischer Form zur Verfügung.

§ 12 Betroffenenrechte und Unterstützung

a. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet der Auftragnehmer das Ersuchen an den Auftraggeber weiter, soweit eine Zuordnung möglich ist. Eine eigenständige Beantwortung erfolgt nur auf Weisung des Auftraggebers oder aufgrund einer gesetzlichen Verpflichtung.
b. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im gesetzlich erforderlichen Umfang bei der Erfüllung von Betroffenenrechten und der Pflichten gemäß Art. 32 bis 36 DSGVO.
c. Unterstützungsleistungen, die über den vereinbarten Leistungsumfang hinausgehen, können nach den vereinbarten Vergütungssätzen abgerechnet werden. Dies gilt nicht, soweit der zusätzliche Aufwand durch einen vom Auftragnehmer zu vertretenden Verstoß gegen diese Vereinbarung verursacht wurde oder zwingendes Recht entgegensteht.

§ 12a Nachweise und Kontrollrechte

a. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten gemäß Art. 28 DSGVO zur Verfügung.
b. Kontrollen erfolgen vorrangig durch Auskünfte, Dokumentationen, Zertifizierungen, Prüfberichte oder vergleichbare geeignete Nachweise.
c. Soweit diese Nachweise für eine angemessene Prüfung ausreichen, besteht kein Erfordernis einer Vor-Ort-Prüfung.
d. Ohne konkreten Anlass sollen keine Vor-Ort-Prüfungen durchgeführt werden. Eine Vor-Ort-Prüfung kommt insbesondere in Betracht, wenn ein konkreter Datenschutzvorfall, begründete Zweifel an der Einhaltung dieser Vereinbarung oder eine Anordnung einer zuständigen Aufsichtsbehörde vorliegen und eine angemessene Prüfung nicht auf andere Weise möglich ist.
e. Erforderliche Vor-Ort-Prüfungen sind grundsätzlich mindestens 14 Werktage vorher anzukündigen, während der üblichen Geschäftszeiten durchzuführen und auf den erforderlichen Umfang zu beschränken. Gesetzlich oder behördlich erforderliche kurzfristigere Prüfungen bleiben unberührt.
f. Prüfungen dürfen nicht zu einem unberechtigten Zugriff auf Daten anderer Kunden, Geschäftsgeheimnisse oder sonstige vertrauliche Informationen des Auftragnehmers führen.
g. Jede Partei trägt ihre eigenen Prüfungskosten. Zusätzlicher personeller Aufwand des Auftragnehmers kann nach den vereinbarten Vergütungssätzen berechnet werden, soweit die Prüfung keinen wesentlichen vom Auftragnehmer zu vertretenden Verstoß ergibt und zwingendes Recht nicht entgegensteht.

§ 13 Abschluss der Verarbeitungsleistungen

Für die Rückgabe, Löschung und weitere Behandlung personenbezogener Daten nach Beendigung der Verarbeitungsleistungen gilt § 7 dieser Vereinbarung.

§ 14 Schlussbestimmungen

a. Werden personenbezogene Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, Insolvenz oder sonstige Maßnahmen Dritter gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich, soweit dies rechtlich zulässig ist.
b. Für diese Vereinbarung gilt deutsches Recht.
c. Für Ansprüche betroffener Personen gilt Art. 82 DSGVO. Im Innenverhältnis der Parteien gelten ergänzend die zwischen ihnen vereinbarten Haftungsregelungen, soweit zwingendes Recht nicht entgegensteht.
d. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Ein elektronisches Format ist ausreichend.
e. Eine Änderung dieser Vereinbarung kommt nicht allein dadurch zustande, dass der Auftragnehmer seine Leistungen nach Zugang einer vom Auftraggeber vorgeschlagenen Vertragsänderung fortsetzt.
f. f. Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, bleiben die übrigen Bestimmungen unberührt. Anstelle der unwirksamen Bestimmung gelten die gesetzlichen Vorschriften.

§ 15 Unterschriften

Ort, Datum	Ort, Datum
- Auftraggeber - - FIRMENNAME -	- Auftragnehmer - - cebra GmbH – new technologies -

Anlage I – Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftragnehmer erbringt insbesondere folgende IT-Leistungen:

- Installation, Administration, Wartung und Support von Servern, PCs, Notebooks, Druckern und sonstigen IT-Systemen
- Installation, Administration und Wartung von Netzwerk-, Router-, Firewall- und NAS-Systemen
- Installation, Administration und Wartung von Telefonanlagen und zugehörigen Komponenten
- Installation, Administration und Wartung von E-Mail-, Archivierungs- und sonstigen Softwarelösungen
- Monitoring und Überwachung von IT-Systemen
- Fernwartung und Remote-Administration
- Datensicherung und Wiederherstellung, soweit entsprechend beauftragt
- Fehleranalyse, Störungsbehebung und IT-Sicherheitsmaßnahmen
- sonstige vom Auftraggeber beauftragte IT-Dienstleistungen

Die Verarbeitung erfolgt ausschließlich, soweit dies zur Erbringung der jeweils beauftragten Leistungen erforderlich ist.

Die Leistungen können vor Ort oder per Fernzugriff erbracht werden.

2. Arten der personenbezogenen Daten

Je nach betreutem System können insbesondere folgende Daten verarbeitet oder eingesehen werden:

- Personenstammdaten
- Kontaktdaten und Kommunikationsdaten
- Beschäftigtendaten
- Kunden- und Interessentendaten
- Vertrags-, Abrechnungs- und Zahlungsdaten
- E-Mail- und sonstige Inhaltsdaten
- Benutzer-, Geräte-, Netzwerk-, Protokoll- und Systemdaten
- Benutzerkennungen, Berechtigungs- und Zugangsdaten
- sonstige personenbezogene Daten, die sich auf den betreuten Systemen befinden

Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO können technisch bedingt oder zufällig zugänglich sein, sind jedoch grundsätzlich nicht Gegenstand einer gezielten Verarbeitung durch den Auftragnehmer.

3. Kategorien betroffener Personen

Betroffene Personen können insbesondere sein:

- Beschäftigte und Bewerber
- Kunden und Interessenten
- Lieferanten und Dienstleister

- Geschäftspartner
- Ansprechpartner
- sonstige Personen, deren personenbezogene Daten auf den betreuten Systemen verarbeitet werden

4. Dauer

Die Dauer der Verarbeitung richtet sich nach § 3 dieser Vereinbarung.

Anlage II – Technische und organisatorische Maßnahmen

Der Auftragnehmer setzt entsprechend Art, Umfang und Risiko der Verarbeitung angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO um.

Die Produktivsysteme des Auftraggebers befinden sich grundsätzlich auf dessen Systemen oder bei eingesetzten Cloud- und Rechenzentrumsanbietern. Eine dauerhafte Speicherung der Produktivdaten des Auftraggebers in den Geschäftsräumen des Auftragnehmers ist grundsätzlich nicht vorgesehen.

Zutritts- und Zugangsschutz

Die Geschäftsräume des Auftragnehmers sind gegen unbefugten Zutritt geschützt.

Der Zugang zu IT-Systemen erfolgt über authentifizierte Benutzerkonten. Administrative Cloud-, RMM- und Fernwartungszugänge werden durch Mehrfaktor-Authentifizierung geschützt, soweit der jeweilige Dienst dies technisch unterstützt.

Arbeitsplätze werden bei Nichtbenutzung gegen unberechtigten Zugriff gesperrt.

Berechtigungen und Vertraulichkeit

Zugriffsrechte werden nach dem Erforderlichkeitsprinzip vergeben und bei Änderung oder Beendigung einer Tätigkeit angepasst oder entzogen.

Personen mit möglichem Zugriff auf personenbezogene Daten sind zur Vertraulichkeit verpflichtet.

IT-Sicherheit

Für den Zugriff auf Kundensysteme eingesetzte Systeme werden regelmäßig mit Sicherheitsupdates versorgt und durch geeignete Firewall- und Schadsoftware-Schutzmaßnahmen abgesichert.

Fernwartungs- und Administrationsverbindungen erfolgen über verschlüsselte oder vergleichbar abgesicherte Verbindungen.

Administrative Zugriffe und sicherheitsrelevante Ereignisse werden protokolliert, soweit dies vom jeweiligen System unterstützt wird.

Umang mit Kundendaten

Personenbezogene Daten des Auftraggebers werden nur im zur Leistungserbringung erforderlichen Umfang verarbeitet.

Vorübergehend auf Systeme des Auftragnehmers übertragene Daten werden nach Wegfall des jeweiligen Zwecks gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten bestehen.

Cloud- und Rechenzentrumsdienste

Soweit Produktivsysteme bei externen Cloud- oder Rechenzentrumsanbietern betrieben werden, werden insbesondere physische Zutrittskontrolle, Stromversorgung, Klimatisierung und infrastrukturelle Sicherheit durch den jeweiligen Anbieter gewährleistet.

Der Auftragnehmer berücksichtigt bei der Auswahl der von ihm eingesetzten Anbieter deren technische und organisatorische Sicherheitsmaßnahmen.

Datensicherung und Wiederherstellung

Datensicherungs- und Wiederherstellungsmaßnahmen für Kundensysteme richten sich nach den jeweils vom Auftraggeber beauftragten Leistungen und vereinbarten Sicherungskonzepten.

Eine Datensicherung außerhalb des vereinbarten Leistungsumfangs ist nicht geschuldet.

Überprüfung

Die technischen und organisatorischen Maßnahmen werden regelmäßig sowie bei wesentlichen technischen Änderungen oder Sicherheitsvorfällen überprüft und bei Bedarf angepasst. Das angemessene Schutzniveau darf dadurch nicht unterschritten werden.

Anlage III

Die nachfolgend aufgeführten Anbieter sind nur insoweit weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO, wie sie im Rahmen der für den Auftraggeber tatsächlich erbrachten Leistungen personenbezogene Daten des Auftraggebers im Auftrag des Auftragnehmers verarbeiten. Die Aufnahme eines Anbieters in diese Anlage stellt daher keine Aussage dar, dass dieser bei jedem Auftraggeber oder bei jeder Leistung als weiterer Auftragsverarbeiter eingesetzt wird.

Der Auftragnehmer hält zu den tatsächlich eingesetzten weiteren Auftragsverarbeitern die erforderlichen Informationen über Identität, Kontaktmöglichkeit, Art der Verarbeitung und gegebenenfalls einschlägige Drittlandgarantien aktuell und stellt diese dem Auftraggeber auf Anfrage zur Verfügung.

Anbieter	Leistung / Einsatzgebiet
octoja GmbH	RMM-, Monitoring- und Fernwartungsdienste, soweit Systeme des Auftraggebers über die Plattform verwaltet werden.
pcvisit Software AG	Fernwartungs- und Remote-Support-Dienste, soweit Systeme des Auftraggebers über pcvisit betreut werden.
netcup GmbH	Cloud- und Hosting-Infrastruktur, soweit der Auftragnehmer dort Systeme oder Dienste für den Auftraggeber betreibt.
Synology Inc. – Synology C2	Cloud-Datensicherungsdienste, soweit entsprechende Sicherungsdienste für den Auftraggeber eingesetzt werden.
Hornetsecurity GmbH	IT-Sicherheits-, E-Mail-, Archivierungs- oder Datensicherungsdienste, soweit entsprechende Dienste für den Auftraggeber eingesetzt werden.

Wasabi Technologies LLC – Wasabi Cloud Storage	Cloud-Speicher- und Datensicherungsdienste, soweit verschlüsselte Sicherungskopien von Systemen oder Daten des Auftraggebers bei Wasabi gespeichert werden. Für die eingesetzten Sicherungsleistungen wird grundsätzlich die Speicherregion Frankfurt am Main (eu-central-2) verwendet.
WORTMANN AG / TERRA CLOUD	Cloud- und Rechenzentrumsdienste, soweit entsprechende Dienste für den Auftraggeber eingesetzt werden.
FISINGER.de	E-Mail-Sicherheits-, Mailfilter-, Hosting- und E-Mail-Archivierungsdienste, insbesondere im Zusammenhang mit MSAVE.de, soweit entsprechende Dienste für den Auftraggeber eingesetzt werden.
Gamma Placetel GmbH	Cloud-Telefonie- und Kommunikationsdienste, soweit hierbei personenbezogene Daten des Auftraggebers verarbeitet werden.
easybell GmbH	Cloud-Telefonie- und Kommunikationsdienste, soweit hierbei personenbezogene Daten im Rahmen einer Auftragsverarbeitung verarbeitet werden.
AGFEO GmbH & Co. KG	Cloud-Telefonie-, Kommunikations- und Telefonbuchdienste, soweit hierbei personenbezogene Daten des Auftraggebers verarbeitet werden.
Microsoft Corporation	Cloud- und IT-Dienste, soweit Microsoft innerhalb der Verarbeitungskette des Auftragnehmers personenbezogene Daten des Auftraggebers verarbeitet.
MailStore Software GmbH	E-Mail-Archivierungs- und zugehörige Support-/Cloud-Dienste, soweit hierbei personenbezogene Daten des Auftraggebers verarbeitet werden.
SecurePoint GmbH	IT-Sicherheits-, Firewall-, VPN- oder Cloud-Dienste, soweit hierbei personenbezogene Daten des Auftraggebers im Auftrag des Auftragnehmers verarbeitet werden.
ELOVADE Deutschland GmbH	Cloud-, Lizenz- und IT-Dienste, soweit über ELOVADE bezogene oder bereitgestellte Dienste personenbezogene Daten des Auftraggebers im Auftrag des Auftragnehmers verarbeiten.
troii Software GmbH	Software- und Cloud-Dienste, insbesondere timr, soweit hierbei personenbezogene Daten des Auftraggebers im Auftrag des Auftragnehmers verarbeitet werden.

Weitere Auftragsverarbeiter werden ausschließlich nach Maßgabe des § 11 dieser Vereinbarung eingesetzt.