Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO

……, ……, ……, ……

- nachstehend Auftraggeber genannt –

KREEVO GmbH, Elstergrund 46, 02979 Elsterheide

- nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Vertragsverhältnis gemachten Angaben.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber i.S.v. Art.4 Nr.2 und Art.28 DSGVO auf Grundlage dieses Auftrags.

Dieser Vertrag gilt für sämtliche gegenwärtigen und künftigen Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und bei denen er personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Bucht der Auftraggeber weitere Leistungen hinzu, gilt dieser Vertrag ohne erneuten Abschluss auch für diese.

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in Ziffer 1 beschriebenen Vertragsverhältnisse ergibt.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO (Art.28 Abs.3 Satz 2 lit.c DS-GVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe Anlage 2). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 Satz 2 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlichder Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach den Art. 15 bis 22 DSGVO, soweit ihm dies möglich ist. Soweit Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft vom Leistungsumfang umfasst sind, setzt er diese nach dokumentierter Weisung des Auftraggebers unmittelbar um.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO und Anlage 2

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

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Vereinbarung gelten Leistungen Dritter, die unmittelbar der Verarbeitung personenbezogener Daten des Auftraggebers dienen. Nicht hierzu gehören reine Nebenleistungen, insbesondere Telekommunikations-, Post-, Transport-, Wartungs- und Benutzerserviceleistungen, sofern dabei keine Verarbeitung personenbezogener Daten im Auftrag erfolgt. Der Auftragnehmer stellt auch bei solchen Nebenleistungen ein angemessenes Datenschutz- und Datensicherheitsniveau sicher.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine schriftliche Genehmigung, die in Anlage 3 benannten Unterauftragnehmer einzusetzen. Der Auftragnehmer informiert den Auftraggeber vor der Hinzuziehung oder Ersetzung eines Unterauftragnehmers in Textform. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Kalendertagen nach Zugang der Information widersprechen. Die Parteien werden in diesem Fall eine datenschutzkonforme Lösung abstimmen.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragnehmer vor Beginn der Verarbeitung durch Vertrag mindestens zu denselben Datenschutzpflichten, die in dieser Vereinbarung für den Auftragnehmer festgelegt sind. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers verantwortlich.

(4) Eine Verarbeitung durch Unterauftragnehmer außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind und der Auftraggeber vorab hierüber informiert wurde.

(5) Die Information nach Absatz 2 erfolgt mindestens vier Wochen vor der beabsichtigten Änderung und nennt Name, Anschrift, Leistung und Ort der Verarbeitung. Sie erfolgt gegenüber den Auftraggebern, deren beauftragte Leistungen von der Änderung betroffen sind. Betrifft eine Änderung ausschließlich Leistungen, die der Auftraggeber nicht beauftragt hat, bedarf es keiner Mitteilung; bucht er eine solche Leistung später hinzu, erhält er mit der Beauftragung die dann gültige Fassung der Anlage 3.

(6) Widerspricht der Auftraggeber fristgerecht und kommt eine einvernehmliche Lösung nicht zustande, ist jede Partei berechtigt, die betroffene Leistung mit einer Frist von einem Monat außerordentlich zu kündigen. Bis zur Klärung setzt der Auftragnehmer den betroffenen Unterauftragnehmer für Daten des Auftraggebers nicht ein. Widerspricht der Auftraggeber nicht innerhalb der Frist, gilt die Änderung als genehmigt.

(7) Wartungs-, Support- und Fernzugriffsleistungen Dritter gelten als Unterauftragsverhältnis, sobald dabei ein Zugriff auf personenbezogene Daten des Auftraggebers möglich ist.

(8) Anlage 3 wird fortgeschrieben, ohne dass es einer Änderung dieses Vertrages bedarf. Die jeweils aktuelle Fassung stellt der Auftragnehmer dem Auftraggeber auf Anfrage zur Verfügung.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchfuhren zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(4) Die Rechte nach den Absätzen 1 und 2 gelten entsprechend für die eingesetzten Unterauftragnehmer. Der Auftragnehmer stellt die erforderlichen Rechte vertraglich sicher und übt sie auf Verlangen des Auftraggebers aus.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

1. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

3. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

(3) Verletzungen des Schutzes personenbezogener Daten meldet der Auftragnehmer dem Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis. Für die Einhaltung der Frist genügt eine erste Meldung mit den verfügbaren Angaben; weitere Informationen reicht er unverzüglich nach. Die Meldung enthält, soweit bekannt, eine Beschreibung des Vorfalls, die betroffenen Datenarten und die ungefähre Zahl der betroffenen Personen, die wahrscheinlichen Folgen sowie die ergriffenen und vorgeschlagenen Maßnahmen. Meldungen gegenüber der Aufsichtsbehörde und den betroffenen Personen obliegen dem Auftraggeber.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird

(3) Weisungsberechtigt sind die vertretungsberechtigten Personen des Auftraggebers sowie die von ihm benannten Ansprechpartner, wie sie im Kundenstamm des Auftragnehmers hinterlegt sind. Der Auftraggeber kann jederzeit in Textform weitere Personen benennen oder Berechtigungen entziehen.

(4) Weisungen, die über die laufende Leistungserbringung hinausgehen, insbesondere die Löschung oder Herausgabe von Daten sowie Änderungen an Zugriffsrechten, nimmt der Auftragnehmer nur von vertretungsberechtigten Personen oder von ausdrücklich hierfür benannten Ansprechpartnern entgegen. In Zweifelsfällen vergewissert er sich auf einem zweiten Weg.

(5) Setzt der Auftraggeber auf seinen Systemen oder Websites Dienste Dritter ein, etwa Karten-, Analyse- oder Videodienste, entscheidet er darüber selbst und ist dafür verantwortlich. Der Auftragnehmer bindet solche Dienste nur auf Weisung ein und weist auf die datenschutzrechtlichen Folgen hin.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer nach Wahl des Auftraggebers sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, herauszugeben oder datenschutzgerecht zu löschen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer bestätigt dem Auftraggeber die Löschung auf Anfrage in Textform.

(3) Datensicherungen werden nach einem festen Rotationsverfahren überschrieben. Darin enthaltene Daten werden nicht gesondert gelöscht; sie werden bis zum Überschreiben gesperrt und nicht mehr für die laufende Verarbeitung verwendet. Die Aufbewahrungsdauer der Sicherungen ergibt sich aus dem jeweiligen Vertragsverhältnis.

(4) Dokumentationen sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Sonstige Vereinbarungen

11.1. Entgelte

Ein Entgelt für diesen Auftrag wird nicht gefordert.

Soweit der Auftraggeber Unterstützung nach Ziffer 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

Soweit der Auftraggeber nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.

Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten

11.2. Vertragsdauer

Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig diese Vereinbarung. Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

11.3. Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland.

11.4. Gerichtsstand

Die Parteien vereinbaren als Gerichtsstand den Sitz des für Hoyerswerda zuständigen Gerichts.

....., ...

(Ort, Datum) (Auftraggeber)

Elsterheide, ...

(Ort, Datum) (Auftragnehmer)

Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO:

Welche Leistungen der Auftragnehmer im Einzelnen erbringt, ergibt sich aus dem jeweiligen Vertragsverhältnis. Die folgende Aufstellung beschreibt den möglichen Umfang; personenbezogene Daten werden jeweils nur verarbeitet, soweit die betreffende Leistung beauftragt ist und solche Daten in den betreuten Systemen anfallen:

- Projektplanung
- Angebotserstellung
- IT-Service und Betreuung
- TK-Service und Betreuung
- Vertrieb von Hardware und Software
- Webhosting
- Webentwicklung
- Webdesign
- Durchführung von Druck- oder Werbemittelproduktionen
- Erstellung von Dokumentationen (IT, TK, WEB)
- IT-Wartungs- und/oder Servicevertrag
- TK-Wartungs- und/oder Servicevertrag
- Web-Wartungs- und/oder Servicevertrag
- Webhostingvertrag

Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung

Art der Daten:

Gegenstand der Zusatzvereinbarung sind folgende Datenarten und -Kategorien

- Mitarbeiterdaten
- Kundendaten
- Lieferantendaten
- Preisinformationen
- Zeiterfassungsdaten

- Protokolldaten
- Benutzerdaten
- Finanzdaten
- Gesundheitsdaten
- Vertragsdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)

Kreis der Betroffenen:

- Mitarbeiter
- Kunden und Interessenten
- Lieferanten
- Dienstleister

Weisungsberechtigte Personen beim Auftragnehmer sind:

Maik Hauska, Geschäftsführer, +49 (0) 3571 - 48 80 80, m.hauska@kreevo.de

Holger Semjank, Geschäftsführer, +49 (0) 3571 - 48 80 80, h.semjank@kreevo.de

Stephan Bartsch, Geschäftsführer, +49 (0) 3571 - 48 80 80, s.bartsch@kreevo.de

Weisungsberechtigte Personen des Auftraggebers sind:

...., ...

.....

.....

.....

.....

.....

.....

(Name, Organisationseinheit, Funktion, Telefon, Email)

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO:

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Kontrollbereich	Umgesetzte Maßnahmen
1. Vertraulichkeit	
Zutrittskontrolle	Zentrale IT-Systeme in einem gesonderten Serverraum; Schließanlage und zusätzlich verschlossener Serverschrank; Zutritt nur für Berechtigte; protokollierte Schlüsselvergabe und Zutritte; gesicherte Büroräume; Besucherbegleitung; Videoüberwachung mit Alarmmeldung.
Zugangskontrolle	Eindeutige Benutzernamen und individuelle Passwörter; Firewall mit IDS/IPS; Virenschutz auf Servern und Clients; gesicherter VPN-Zugang für Heimarbeitsplätze; verpflichtende IT-Sicherheitsrichtlinie einschließlich Bildschirmsperre; verschlüsselter Extranet-Zugang per SSL.
Zugriffskontrolle	Genehmigung und zentrale Vergabe von Systemberechtigungen im Check-in-Prozess; Entzug von Berechtigungen und Rückgabe von Systemen und Datenträgern im Check-out-Prozess; Datei- und Netzwerkzugriffe über Active Directory und definierte Berechtigungsgruppen; Aktenvernichtung durch lokalen, nach DIN EN ISO 9001 zertifizierten Dienstleister in Sicherheitsstufe 4.
Trennungskontrolle	Auftrags- und kundenbezogene Trennung der Daten im ERP-System.
Verschlüsselung	Transportverschlüsselung für Websites, E-Mail und Fernwartung; verschlüsselte Datensicherungen; Übermittlung von Zugangsdaten über einen verschlüsselten Einmal-Link oder ein verschlüsseltes Archiv mit Kennwort auf getrenntem Weg.
2. Integrität	
Weitergabekontrolle	Weitergabe von Kundendaten für Fehleranalyse und Support nur im Rahmen des Auftrags; verschlüsselte Übertragung; getrennte Übermittlung von Passwort und Daten; Unterweisung und Verpflichtung der Beschäftigten zum datenschutzkonformen Umgang mit personenbezogenen Daten.
Eingabekontrolle	Protokollierung durch Log-Dateien auf zentralen Serversystemen; anlassbezogene Auswertung.
3. Verfügbarkeit und Belastbarkeit	
Verfügbarkeitskontrolle	Serverbetrieb in einem gesonderten Raum mit USV, Überspannungsschutz, Rauchmelder, Klimatisierung und Temperaturüberwachung; regelmäßige Datensicherungen und Prüfung der Rückspielbarkeit; verschlüsselte Sicherung in einem anderen Brandabschnitt; Wartungsverträge für wichtige Systeme; Notfallhandbuch.
4. Regelmäßige Überprüfung, Bewertung und Evaluierung	
Datenschutz durch Technikgestaltung	Datenschutzfreundliche Voreinstellungen bei der Softwareentwicklung gemäß Art. 25 Abs. 2 DS-GVO.
Incident Response	Incident-Response-Management ist vorhanden.
Auftragskontrolle	Vertragliche Regelung mit eingesetzten IT-Dienstleistern; regelmäßige Datenschutzunterweisung der Beschäftigten; Verfahrensanweisungen und Benutzerrichtlinien zur Auftragsverarbeitung; Zweckbindung in den AGB.
Weitere Maßnahmen	Verpflichtung aller Beschäftigten auf Datenschutz und Vertraulichkeit; Clean-Desk-Policy.

Anlage 3 – Unterauftragnehmer

Für die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers setzt der Auftragnehmer die nachfolgend aufgeführten Unterauftragnehmer ein. Die Genehmigung und das Änderungsverfahren richten sich nach Ziffer 6 dieser Vereinbarung.

Verzeichnis der bei Vertragsschluss genehmigten Unterauftragnehmer

Unterauftragnehmer, deren Leistung mit „Nur bei …“ gekennzeichnet ist, kommen ausschließlich bei Beauftragung der jeweiligen Leistung zum Einsatz und gelten mit deren Beauftragung als genehmigt.

Unterauftragnehmer / Anschrift	Leistung	Datenkategorien / Betroffene	Ort der Verarbeitung
NinjaOne GmbH Alexanderstraße 1 10178 Berlin	Remote-Monitoring und -Management (RMM), Endpoint- und Patch-Management, Fernwartung	Geräte-, System-, Benutzerbezugs-, IP-, Ereignis-, Konfigurations- und Protokolldaten; Beschäftigte und sonstige Nutzer der betreuten Systeme	Deutschland/EU; weitere Orte gemäß gültigem Anbieter-DPA
Hornetsecurity GmbH Am Listholze 78 30177 Hannover	E-Mail-Sicherheit, Archivierung, Microsoft-365-Backup, DMARC- und Compliance-Dienste	E-Mail-Inhalte und -Metadaten, Anhänge, Konten-, Kommunikations-, Sicherungs-, Sicherheits- und Protokolldaten; Beschäftigte und Kommunikationspartner	Deutschland/EU; weitere Orte gemäß jeweils gültigem Anbieter-AVV
Securepoint GmbH Bleckeder Landstraße 28 21337 Lüneburg	Firewall-, Antivirus- und MDM-Management sowie zugehörige Cloud- und Supportdienste	Geräte-, Benutzerbezugs-, IP-, Netzwerk-, Sicherheits-, Konfigurations- und Protokolldaten; Beschäftigte und sonstige Nutzer der betreuten Systeme	Deutschland/EU; weitere Orte gemäß jeweils gültigem Anbieter-AVV
Synology GmbH Grafenberger Allee 295 40237 Düsseldorf	Active Insight: cloudbasiertes Monitoring von NAS-Systemen, Zustands- und Ereignisanalyse	Gerätekennungen, Systemzustand, Leistungs-, Speicher-, Konfigurations-, IP-, Ereignis- und Telemetriedaten; Beschäftigte und Systemnutzer mit technischem Bezug	Deutschland/EU; weitere Orte gemäß jeweils gültigem Anbieter-DPA
Sophos Limited The Pentagon Abingdon Science Park Abingdon, Oxfordshire OX14 3YP Vereinigtes Königreich	Zentrales Management und Monitoring von Firewall- und Antivirus-Lösungen, Bedrohungsanalyse, Sicherheits-, Ereignis- und Supportdienste	Geräte-, Benutzerbezugs-, IP-, Netzwerk-, Sicherheits-, Ereignis-, Konfigurations-, Telemetrie- und Protokolldaten; Beschäftigte und sonstige Nutzer der betreuten Systeme	Deutschland/EU; weitere Orte gemäß jeweils gültigem Anbieter-DPA
TERRA CLOUD GmbH, Hankamp 2, 32609 Hüllhorst	Bereitstellung und Betrieb virtueller Server- und Hosting-Infrastruktur für Voice-IP-Kommunikations-anlagen einschließlich	Benutzer-, Konten-, Nebenstellen-, Rufnummern-, Konfigurations-, Verbindungs-, Kommunikations-, Protokoll-, Voicemail- und gegebenenfalls Aufzeichnungsdaten;	Deutschland

Unterauftragnehmer / Anschrift	Leistung	Datenkategorien / Betroffene	Ort der Verarbeitung
	Speicher-, Sicherungs- und Infrastruktur-leistungen	Beschäftigte und Kommunikationspartner	
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server- und Hosting-Infrastruktur, Webhosting sowie Speicher- und Sicherungsdienste (Storage Box)	sämtliche in den betreuten Systemen gespeicherten Daten, Protokoll- und Zugriffsdaten; Beschäftigte, Kunden und Nutzer des Auftraggebers	Deutschland
c-entron / NEXOWARE Systems GmbH, Einsteinstr. 59, 89077 Ulm	Hersteller-Support für das Warenwirtschafts- und Ticketsystem, in dem Vorgänge und technische Dokumentation geführt werden	Stamm-, Kontakt-, Vertrags-, Vorgangs- und Dokumentationsdaten; Ansprechpartner und Beschäftigte	Deutschland
Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Dublin 18, Irland	E-Mail- und Kommunikationsdienste (Microsoft 365), über die die Korrespondenz mit dem Auftraggeber geführt wird	Kommunikationsinhalte und -metadaten, Kontakt- und Kontodaten; Beschäftigte und Kommunikationspartner	EU (Microsoft EU Data Boundary); Konzernmutter USA, abgesichert über EU-US Data Privacy Framework und Standardvertragsklauseln
mySites.guru, Blue Flame Digital Solutions Ltd., Jersey	Nur bei Websitebetreuung: Wartung, Updates, Überwachung und Sicherung der betreuten Websites	Inhalts-, Benutzer-, Protokoll- und Sicherungsdaten der Website; Redakteure und Websitebesucher	Vereinigtes Königreich (London); Unterauftragnehmer in der EU und den USA, abgesichert über Standardvertragsklauseln und das EU-US Data Privacy Framework
pcvisit Software AG, Manfred-von-Ardenne-Ring 20, 01099 Dresden	Nur im Einzelfall: Fernwartungssitzungen	Bildschirminhalte während der Sitzung, Geräte- und Verbindungsdaten	Deutschland
CopyThek Lausitz GmbH, Ackerstraße 8, 02977 Hoyerswerda (Tochtergesellschaft des Auftragnehmers)	Unterstützung bei Betreuung, Service und Verwaltung; gemeinsame Nutzung der IT-Systeme	Stamm-, Vorgangs- und Kommunikationsdaten; Ansprechpartner und Beschäftigte	Deutschland

Änderungsmitteilung: Änderungen dieses Verzeichnisses werden dem Auftraggeber vor ihrem Wirksamwerden in Textform mitgeteilt, soweit seine beauftragten Leistungen betroffen sind. Die Mitteilung bezeichnet mindestens den Unterauftragnehmer, die Leistung, den Verarbeitungsort und gegebenenfalls die Grundlage eines Drittlandtransfers. Das Widerspruchsrecht nach Ziffer 6 bleibt unberührt.

Nicht jeder Dienstleister ist ein Unterauftragnehmer.

In dieser Liste stehen deshalb nicht:

- Lieferanten von Hardware, Software und Lizenzen sowie Post- und Paketdienste, soweit sie keinen Zugriff auf personenbezogene Daten des Auftraggebers erhalten
- Telekommunikationsanbieter, mit denen der Auftraggeber selbst einen Vertrag schließt
- Systeme, die der Auftragnehmer selbst betreibt, etwa für Dokumentation, Passwortverwaltung, Überwachung und Statistik; hier wird kein Dritter beauftragt
- Abrufe von Mess- und Sicherheitsdaten zu den betreuten Websites, bei denen nur gelesen wird und die Auswertung ausschließlich beim Auftragnehmer erfolgt

Stand: 06.10.2026