**Vereinbarung zur Auftragsdatenverarbeitung
nach Art. 28 Abs. 3 DSGVO**

**Kunde**

- 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.

**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, Sperrung 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) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

**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**

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

**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.

**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.

**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

**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 sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

(3) 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, 11.06.2018

……………………………………………………….. …………………………………………………….

(Ort, Datum) (Auftragnehmer)

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

**Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen (ganz oder in Teilen):**

* 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 und Anlage**

* **Vertraulichkeit**
	+ Zutrittskontrolle

		- Alle zentralen IT-Systeme der KREEVO GmbH befinden sich in einen speziell dafür vorgesehen Serverraum
		- Alle Daten werden innerhalb Deutschlands gespeichert und verarbeitet.
		- Der Serverraum ist durch eine Schließanlage sowie durch ein extra Schloss am Serverschrank abgesichert und nur berechtigte Personen haben Zutritt.
		- Der Zutritt zum Serverraum wird protokolliert, die Schlüsselausgabe erfolgt nur per Protokoll (Angabe von Grund, Zeit, Datum)
		- Die Büroräume der KREEVO GmbH sind durch eine Schließanlage gesichert. Nur die dafür berechtigten Personen haben Schlüssel zu ihren Büros
		- Wenn ein Besucher bzw. Gast die KREEVO GmbH betritt, wird dieser von einen Mitarbeiter begleitet
		- Der Zugang zur KREEVO GmbH, die Büroräume und der Serverraum sind durch eine Videoüberwachung mit Alarmmeldung gesichert
	+ Zugangskontrolle

		- Für alle IT-Systeme im Unternehmen werden eindeutige Benutzernamen und individuelle Passwörter vergeben
		- Das Unternehmensnetzwerk ist durch eine Firewall vom Internet geschützt
		- Die Firewall verfügt über ein integriertes IDS / IPS - Verfahren
		- Server als auch Clients sind mit einem angemessenen Virenschutz ausgestattet
		- Der Zugang von einem Heimarbeitsplatz auf IT-Systeme des Unternehmens geschieht mittels einer gesicherten VPN-Verbindung.
		- Die Mitarbeiter sind dazu verpflichtet unsere IT-Sicherheitsrichtlinie umzusetzen (z.B: Bildschirm wird gesperrt und mit Passwort gesichert bei verlassen des Arbeitsplatzt)
		- Zugang zum Extranet erfolgt über individuelle Benutzernamen und Passwörter, die Verbindung erfolgt verschlüsselt (SSL)
	+ Zugriffskontrolle

		- Im Rahmen des formularbasierten Check-In Prozesses werden vom Vorgesetzten die einzelnen Systemberechtigungen für neue Mitarbeiter genehmigt und zentral von der Personal- bzw. IT-Abteilung vergeben
		- Durch den formularbasierten Check-Out Prozess wird sichergestellt, dass beim Ausscheiden eines Mitarbeiters alle Berechtigungen entzogen und alle IT-Systeme sowie Datenträger zurückgegeben werden.
		- physische Daten und Akten werden durch einen lokalen Dienstleister zertifiziert nach DIN EN ISO 9001 entsprechend Bundesdatenschutzgesetz in der Sicherheitsstufe 4 vernichtet
		- Der Datei und Netzwerkzugriff erfolgt über das Active Directory und wird vom Administrator eingestellt. Die Geschäftsführer bestimmen die Berechtigungsgruppe
	+ Trennungskontrolle

		- Durch das ERP-System werden die Daten Auftragsbezogen, nach Kunden getrennt verwaltet
* **Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**
	+ Weitergabekontrolle

		- Eine Weitergabe von Kundendaten im Rahmen von Fehleranalysen und Supporttätigkeiten erfolgt nur im Rahmen des Auftrages, der Austausch der Daten erfolgt über ein eine verschlüsselte verbind die Daten werden verschlüsselt übertragen (Passwort und Daten werden getrennt übermittelt)
		- Alle Mitarbeiter sind i.S.d. Art.32 Abs.4 DS-GVO unterwiesen und verpflichtet, den Datenschutzkonformen Umgang mit personenbezogenen Daten sicher zu stellen
	+ Eingabekontrolle

		- Alle zentralen Server-Systeme erstellen Log-Files, die anlassbezogen ausgewertet werden
* **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

	+ Verfügbarkeitskontrolle

		- Alle Server von KREEVO GmbH stehen beim IT-Dienstleister in einem speziellen Raum, welcher mittels einer unterbrechungsfreien Stromversorgung (USV) mit Überspannungsschutz, Rauchmelder, einer Klimatisierung und automatischen Sensoren zur Temperaturüberwachung ausgestattet ist
		- Darüber hinaus werden regelmäßig Datensicherungen vorgenommen und auf Rückspielbarkeit verifiziert.
		- Die Datensicherung wird in einem anderen Brandabschnitt verschlüsselt abgelegt.
		- Für wichtige Systeme existieren Wartungsverträge, welche die externe Unterstützung bei Problemen regeln.
		- Die KREEVO GmbH verfügt über ein Notfallhandbuch.
* **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art 25 Abs. 1 DS-GVO)**
	+ - Datenschutzfreundliche Voreinstellungen werden bei der Softwareentwicklung berücksichtigt (Art. 25 Abs. 2 DS-GVO)
		- Incident-Response-Management ist vorhanden
	+ Auftragskontrolle

		- Es existiert ein Auftrag oder Dienstleistungsvertrag mit dem IT-Dienstleister
		- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers
		- Die AGB beinhalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers

**Der Auftragnehmer verpflichtet sich zur Einhaltung folgender weiteren technischen und organisatorischen Maßnahmen zur Datensicherheit:**

* Verpflichtungserklärung aller Mitarbeiter zum Datenschutz und Datengeheimnis
* Clean Desk Policy

**Anlage 3 - Unterauftragnehmer**

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

* Webhosting:

	+ Hetzner Online GmbH (Server Hosting)

<https://www.hetzner.com/AV/TOM.pdf>

Verschiedene Druckereien oder Werbetechnik-Firmen, die im Auftrag der KREEVO GmbH Druckaufträge durchführt. Neben den kundenspezifischen Druckdaten werden i.d.R. Adressdaten, Telefondaten und Name des Ansprechpartners mitgeteilt, um einen direkten Versand an den Kunden zu ermöglichen.