

Zwischen dem ITEXIA Kunden (Auftraggeber) und der ITEXIA GmbH (Auftragnehmer) wird nachfolgender Vertrag geschlossen.

Präambel

- (1) Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Nutzung gemäß §1 Absatz 2 in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.
- (2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Vertrags. Eine Kündigung des Vertrages bewirkt automatisch die Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

§1 Gegenstand, Dauer und Spezifizierung des Auftrags

- (1) Die Nutzung der Software ITEXIA erfolgt als SaaS-Lösungen (Cloud) auf den Servern des Auftragnehmers. Gegenstand und Laufzeit dieser Vereinbarung ist im Vertrag definiert. Für die Beurteilung der Zulässigkeit der Datenerhebung / -verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsdatenverarbeitung der Nutzung der Software ITEXIA ergeben. Die Erhebung bzw. Verarbeitung oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung im Zusammenhang mit der Erbringung von Servicedienstleistungen für die Software ITEXIA.
- (2) Produktbeschreibung:
Wir helfen Unternehmen den hohen Aufwand der manuellen Inventarisierung von Mobiliar, IT-Equipment, Maschinen, etc. zu beseitigen, indem wir die Inventarverwaltung digitalisieren und automatisieren. Das Inventar wird mit maschinenlesbaren Etiketten versehen (Barcode, QR-Code oder RFID-Tag). Bei der Inventur werden die Etiketten mit einem mobilen Datenerfassungsgerät (Smartphone, Industriescanner oder RFID Reader) in Verbindung mit der App ITEXIA MDT oder App ITEXIA Smartphone gescannt und zum Datenbestand hinzugefügt. Damit schaffen wir einen einfachen Überblick über alle Gegenstände (Inventare) im Unternehmen. Die geprüften Inventurdaten können dann aus der Software ITEXIA direkt in bestehende Dritt-System übertragen werden. Der Inventarverantwortliche erhält über seinen Zugang einen aktuellen Soll-Ist-Vergleich und kann auftretende Abweichungen selbst in der Software ITEXIA bearbeiten. Änderungs- und Abgangsprotokolle sind nicht mehr nötig.
- (3) Kreis der Betroffenen können u.a. sein,
 - Personal einschließlich Freiwilliger, Beauftragte, Zeitarbeitskräfte und Aushilfen
 - Studenten und Schüler
- (4) Diese Vereinbarung regelt die Maßnahmen, die Art. 28 DS-GVO zwischen Auftraggeber und Auftragnehmer zum Schutz personenbezogener Daten verlangt.

Art der Auftraggeber-Daten	Arten der Verarbeitung	Zweck der Datenerhebung, -verarbeitung oder -nutzung	Kreis der Betroffenen
Name, Vorname Technische Daten zu Geräten mit ggf. Personenbezug, E-Mail-Adresse	Zuordnung zum jeweiligen Inventar/ Gegenstand	Der Auftragnehmer erbringt für den Auftraggeber Prüftätigkeiten, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann. Zur Authentifizierung und Berechtigung	Auftraggeber/ Mitarbeiter

§2 Anwendungsbereich und Verantwortlichkeit

- (1) Der Auftragnehmer verarbeitet ggf. personenbezogene Daten im Auftrag des Auftraggebers gemäß dem Vertrag und dessen Leistungsbeschreibung und wie in dieser Vereinbarung konkretisiert. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.
- (2) Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte

Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Die begründeten Kosten sind durch den Auftraggeber zu tragen.

Weisungsempfänger beim Auftragnehmer sind:

- Die beauftragende Fachabteilung oder Einzelpersonen:
Customer Success Management (CSM)
- (bzw. separat benannter Stellvertreter/Nachfolger)
Steffen Prasse

§ 3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf personenbezogene Daten von betroffenen Personen nur im Rahmen des Auftrages, näher bestimmt durch den Vertrag und diese Vereinbarung, und der dokumentierten Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a) DS-GVO vor. In einem solchen Ausnahmefall informiert der Auftragnehmer den Auftraggeber von seiner gesetzlichen Verpflichtung, sofern er gesetzlich nicht daran gehindert ist.
- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DS-GVO genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Des Weiteren sind Maßnahmen zu treffen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen unverzüglich wiederherzustellen sowie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu implementieren. Zu den zu ergreifenden Maßnahmen gehören auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten, soweit dies für die Gewährleistung eines angemessenen Schutzniveaus erforderlich ist.
- (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 und dem Auftraggeber unverzüglich mitzuteilen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. B DS-GVO)

1.1. Zutrittskontrolle

Die Rechenzentrumsgebäude der Deutschen Telekom AG sind durch Sicherheitsschlösser, vergitterte Fenster und Rollos gesichert. Der Zutritt über die vorgesehenen Zutrittswege ist nur autorisierten Personen mit Magnetkarte und Schlüssel möglich. Darüber hinaus sind die Zutrittswege durch Wachschatz, Video- und Alarmanlagen gesichert. Zutrittsberechtigte Mitarbeiter sind organisatorisch festgelegt, Magnetkarten und Schlüssel werden nur entsprechend der Organisationsanweisung vergeben. Über den Zutritt werden Anwesenheitslisten geführt, Regelungen für Fremdpersonal und Richtlinien zur Begleitung von Gästen sind vorhanden. Es erfolgt eine Zutrittskontrolle zu den Büroräumen des Auftragnehmers durch verschiedene Schlüssel. Eine Dokumentation und Vergabe von Schlüsseln erfolgen. Eine Besucherkontrolle und Abholung und Begleitung durch Mitarbeiter besteht. Betriebsfremde Personen werden in den Räumen des Auftragnehmers begleitet.

1.2. Zugangskontrolle

Der Zugang zu Systemen ITEXIA erfolgt mit Authentifizierung durch individuelle Benutzererkennung und Passwort. Berechtigungen werden nach einem Zugangsberechtigungskonzept vergeben. Laufende aktualisierte Systeme gegen Schadsoftware (z.B. Virenschutz) für Server und Arbeitsplatzrechner sind im Einsatz.

Die Systeme sind gegen unberechtigten Zugang durch eine Firewall gesichert. Passwortgeschützte Bildschirmschoner schützen auch bei vorübergehender Abwesenheit eines Mitarbeiters des Auftragnehmers vor Einsicht Unbefugter. Datensicherungsträger werden nur in gesicherten Räumen gelagert. Es erfolgt eine kontrollierte Vernichtung von Datenträgern und elektronischen Daten des Auftraggebers.

1.3. Zugriffskontrolle

Berechtigungen sind in der Software ITEXIA festgelegt, differenzierte Zugriffe und differenzierte Berechtigungen werden festgelegt. Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch) sind getrennt. Der Zugriff entsprechend Berechtigung wird auch bei Verfahren zur Wiederherstellung von Daten aus Backups gewährt. Fernwartungen werden mit eindeutiger Benutzererkennung vorgenommen. Alle Benutzer des Auftragnehmers haben eindeutige Benutzerkennungen. Regelung zum Passwortgebrauch bestehen und sind

bekannt. Ein regelmäßiger Passwortwechsel wird erzwungen und ausgeschiedenen Mitarbeiter werden umgehend gesperrt.

1.4. Trennungskontrolle (Trennungsgebot)

Es erfolgt eine Trennung der Daten des Auftraggebers von eigenen Daten / anderen Auftragsdaten, zumindest durch die Trennung im Rahmen der Berechtigungsverwaltung (Mandanten). Eine Trennung von Test- und Produktivsystem findet bei dem Auftraggeber statt.

1.5. Pseudonymisierung

Eine anonymisierte oder pseudonymisierte Form der Daten erfolgt nicht.

2. Integrität (Art. 32 Abs. 1 lit. B DS-GVO)

2.1. Weitergabekontrolle

Alle Mitarbeiter des Auftragnehmers werden über das Datengeheimnis informiert. Soweit erforderlich werden die Daten gegen Zugriffe auf Netzwerkebene geschützt, Daten verschlüsselt und Schnittstellen gegen unbefugten Datenexport gesichert.

2.2. Eingabekontrolle

Es wird - auf Wunsch des Auftraggebers - durch individuelle Zugriffskonten des Auftragnehmers beim Kunden im Rahmen der Datensicherung der Kundensysteme gewährleistet, dass überprüft werden kann, ob und von wem personenbezogene Daten durch den Auftragnehmer eingegeben, verändert oder entfernt worden sind.

3. Verfügbarkeit und Belastbarkeit (Art. 32. Abs. 1 lit. b DS-GVO)

3.1. Verfügbarkeitskontrolle

Regelmäßige Rücksicherungen der Systeme des Auftragnehmers werden getestet. Der Auftraggeber ist für die Sicherung der Daten auf seinen Systemen selbst verantwortlich, kann sich jedoch zur technischen Umsetzung der Unterstützung des Auftragnehmers bedienen. Ein ausreichender Viren- und Firewall Schutz ist bei dem Auftragnehmer umgesetzt. Die Lagerung der Datensicherungsträger mit Daten des Auftraggebers findet in einem anderen Brandabschnitt als der Betrieb der zu sichernden Systeme statt. Das Hosting für die SaaS-Lösung erfolgt auf den Servern der T-Systems International GmbH. Es erfolgt der Einsatz von aktuellen Sicherheitsupdates auf Systemen des Auftragnehmers.

3.2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Der Auftragnehmer stellt die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall sicher.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32. Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1. Datenschutz-Management

- Datenschutzbeauftragter ist benannt
- regelmäßige Kontrolle durch den Datenschutzbeauftragten
- Beschäftigten sind zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet.

4.2. Datenschutzfreundliche Voreinstellungen

Der Auftraggeber behält sich Maßnahmen vor, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

4.3. Incident-Response-Management

Ein Vorfalreaktionsplan ist nicht vorhanden.

- (4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.
- (5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die in der Vereinbarung getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab..
- (6) Der Auftragnehmer nennt dem Auftraggeber – auf Verlangen - den Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Datenschutzfragen.
- (7) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind, wie z.B. seiner Pflicht, einen Datenschutzbeauftragten zu bestellen, soweit vom Gesetz vorgeschrieben.

- (8) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.
- (9) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Servicevertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.
- (10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

§ 4 Rechte und Pflichten des Auftraggebers

- (1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der einschlägigen Datenschutzgesetze, insbesondere bezogen auf die Verpflichtungen als Auftraggeber für die Rechtmäßigkeit der Vergabe der Verarbeitung personenbezogener Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich.
- (2) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeiteten Daten ein angemessenes Schutzniveau bieten.
- (3) Die Weisungen werden anfänglich durch den Vertrag und diese Vereinbarung festgelegt und können vom Auftraggeber in schriftlicher Form oder Textform an, die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (sogenannte Einzelweisung). Änderungen des Verarbeitungsgegenstandes oder Verfahrensänderungen sind gemeinsam abzustimmen und entsprechend Satz1 schriftlich oder in Textform vom Auftraggeber festzulegen. Die letzte Entscheidungsbefugnis liegt beim Auftraggeber.
- (4) Der Auftraggeber hat das Recht, insbesondere in folgendem Umfang zusätzliche Weisungen gegenüber dem Auftragnehmer zu erteilen:
 - Im Hinblick auf die Erfüllung des Vertrages
 - Im Hinblick auf zusätzlichen Datensicherungsmaßnahmen
 - Im Hinblick auf das Vorgehen bei Datenschutzverstößen
- (5) Der Auftragnehmer nennt dem Auftraggeber - auf Verlangen - den Ansprechpartner für die im Rahmen dieser Vereinbarung anfallende Datenschutzfragen.
- (6) Für den Fall, dass sich die weisungsberechtigten Personen oder die primären Kontaktpersonen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich mitteilen.
- (7) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (8) Im Falle einer Inanspruchnahme einer Vertragspartei durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO in Bezug auf die Datenverarbeitung nach dieser Vereinbarung oder in deren Zusammenhang, verpflichtet sich die in Anspruch genommene Vertragspartei, die andere Vertragspartei unverzüglich zu informieren. Die Vertragsparteien werden sich bei der Abwehr des Anspruchs gegenseitig unterstützen.

§ 5 Anfragen Betroffener

- (1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.
- (2) Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

§ 6 Kontrollpflichten

Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und so dann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis.

- Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen
- oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.
- Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen mitwirkt. Mehraufwände sind durch den Auftraggeber zu tragen.

§ 7 Subunternehmer

- (1) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in Absatz (3) aufgeführten Unternehmen als Subunternehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Subunternehmer gilt die Einwilligung für das Tätigwerden als erteilt.
- (2) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit den aufgeführten Leistungen unterbeauftragt. Dies bedarf der ausdrücklichen Zustimmung des Auftraggebers (mind. Textform).
- (3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung eines Subunternehmers durchgeführt, nämlich:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
Open Telekom Cloud der Deutschen Telekom AG T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main	Infrastructure-as-a-Service, Hosting
HubSpot Germany GmbH, Koppenstrasse 93, 10243 Berlin, Germany	CRM-Provider

- (4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieser Vereinbarung. Eine etwaige Prüfung durch den Auftraggeber beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragnehmer.
- (5) Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
- (6) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 8 Salvatorische Klausel, Schriftformklausel, Rechtswahl

- (1) Sollten einzelne Teile dieser Vereinbarung teilweise unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung nicht. Anstelle der unwirksamen Bestimmungen werden die Vertragsparteien eine angemessene Regelung vereinbaren, die rechtlich zulässig ist und in ihrem wirtschaftlichen Gehalt der ursprünglichen Bestimmung am nächsten kommt.
- (2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Servicevertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
- (4) Es gilt deutsches Recht. Als Gerichtsstand wird Dresden (Deutschland) vereinbart.