## ANHANG zur DATENVERARBEITUNG 1

Dieser ANHANG zur DATENVERARBEITUNG (hiernach ANHANG) wird am GÜLTIGKEITSDATUM geschlossen von und zwischen:

KUNDE per Definition gemäß LEISTUNGSBESCHREIBUNG

– hiernach bezeichnet als „**DATENVERANTWORTLICHER**“ –

*oder*

Firma von Datasite per Definition gemäß LEISTUNGSBESCHREIBUNG

– hiernach bezeichnet als „**DATENVERARBEITER**“ –

Hiernach einzeln als „**PARTEI**“ und gemeinsam als die „**PARTEIEN**“ bezeichnet

**Präambel:**

(A) Die PARTEIEN sind eine VEREINBARUNG eingegangen, in welcher die zu erbringenden DIENSTE (Definitionen in ABSCHNITT 1 weiter unten) festgelegt sind. Im Rahmen der Leistungserbringung durch den DATENVERARBEITER können PERSONENBEZOGENE DATEN vom DATENVERANTWORTLICHEN an den DATENVERARBEITER übertragen werden.

(B) Im Falle eines Widerspruchs zwischen den Bestimmungen in diesem ANHANG und den Bestimmungen in der VEREINBARUNG hat/haben die Bestimmung(en) in diesem ANHANG Vorrang. Begriffe mit durchgehenden Großbuchstaben, die nicht in diesem ANHANG definiert sind, werden in der VEREINBARUNG definiert.

(C) Um die Einhaltung der Verarbeitungspflichten gemäß der DATENSCHUTZREGELUNGEN in ihrer jeweils gültigen Fassung durch die PARTEIEN zu gewährleisten, stimmen die PARTEIEN hiermit Folgendem zu:

**1. Definitionen**

**1.1.** „**ZUSATZ**“ bedeutet den beiliegenden Zusatz, der einen Bestandteil dieses ANHANGS bildet;

**1.2.** „**DATENSCHUTZLAND**“ oder „DATENSCHUTZLÄNDER“ bedeutet ein Land oder Länder, in dem/denen Gesetze zu Datenschutz, Datensicherheit oder Informationssicherheit in Kraft sind, welche den Umfang mit persönlichen bzw. privaten Informationen oder PERSONENBEZOGENEN DATEN regeln, darunter der Europäische Wirtschaftsraum, Brasilien, Hongkong, Australien, Singapur, Kanada, das Vereinigte Königreich und die Schweiz;

**1.3.** „**DATENSCHUTZREGELUNGEN**“ bedeutet die relevanten nationalen Gesetze, welche die VERARBEITUNG PERSONENBEZOGENER DATEN in DATENSCHUTZLÄNDERN regeln, einschließlich, aber ohne Beschränkung auf Gesetze und Bestimmungen zum Datenschutz und zur Informationssicherheit in ihrer jeweils gültigen Fassung;

**1.4.** „**BETROFFENE PERSON**“ bedeutet eine identifizierte oder identifizierbare natürliche Person, deren PERSONENBEZOGENE DATEN der VERARBEITUNG unterliegen; eine identifizierbare Person ist eine Person, die direkt oder indirekt per Verweis über eine Kennung wie Name, Identifikationsnummer, Standortdaten, eine Online-Kennung oder mindestens einen spezifischen Faktor bezüglich physischer, physiologischer, genetischer, mentaler, ökonomischer, kultureller oder sozialer Identität identifiziert werden kann;

**1.5.** „**INFORMATIONSSICHERHEITSVORFALL**“ bedeutet jegliche Übertragung, jeden Zugriff und jede Offenlegung durch bzw. gegenüber Dritten oder die VERARBEITUNG unter Nichteinhaltung dieses ANHANGS oder der DATENSCHUTZREGELUNGEN, der/die in jedem Fall direkt oder indirekt die Vertraulichkeit, Integrität oder Authentizität PERSONENBEZOGENER DATEN beeinträchtigt;

**1.6.** „**PRIVACY SHIELD**“ meint das EU-US Privacy Shield Framework, das am 1. August 2016 in Kraft trat, sowie das Swiss-US Privacy Shield Framework, das am 12. April 2017 in Kraft trat.

**1.7.** „**VEREINBARUNG**“ bedeutet die LEISTUNGSBESCHREIBUNG und die ALLGEMEINEN GESCHÄFTSBEDINGUNGEN zwischen dem DATENVERANTWORTLICHEN und dem DATENVERARBEITER;

**1.8.** „**PERSONENBEZOGENE DATEN**“ bedeutet jegliche Informationen mit Bezug auf eine BETROFFENE PERSON in den INHALTEN.

**1.9.** „**VERARBEITEN**“, „**VERARBEITUNG**“ oder „**VERARBEITET**“ bedeutet jeglichen Vorgang oder eine Reihe von Vorgängen, die mit PERSONENBEZOGENEN DATEN durchgeführt werden, unabhängig von deren Automatisierung, darunter beispielsweise Erfassung, Aufzeichnung, Organisation, Strukturierung, Speichern, Anpassung oder Änderung, Abruf, Aufruf, Nutzung, Offenlegung durch Übertragung, Verbreitung oder sonstige Bereitstellung, Ausrichtung oder Kombination, Sperrung, Löschung oder Zerstörung;

**1.10** „**DIENSTE**“ bedeutet die Erbringung von DIENSTEN, die in der VEREINBARUNG und diesem ANHANG beschrieben werden;

**1.11** „**BESONDERE DATENKATEGORIEN**“ meint PERSONENBEZOGENE DATEN, welche Aufschluss über ethnische Herkunft, politische Überzeugungen, religiöse oder philosophische Einstellung, Gewerkschaftszugehörigkeit, genetische Daten und biometrische Daten zur eindeutigen Identifikation einer natürlichen Person geben sowie PERSONENBEZOGENE DATEN hinsichtlich Gesundheit, Sexualleben oder sexueller Orientierung;

**2. Verarbeitungsaktivitäten**

Der DATENVERANTWORTLICHE ist allein für die Genauigkeit, Qualität und Legalität der VERARBEITUNG PERSONENBEZOGENER DATEN zuständig und hat für alle eingeladenen BENUTZER die geltenden DATENSCHUTZREGELUNGEN einzuhalten. Der DATENVERARBEITER stimmt zu, die PERSONENBEZOGENEN DATEN zu VERARBEITEN, um in Übereinstimmung mit diesem ANHANG und der VEREINBARUNG DIENSTE gemäß den schriftlichen Anweisungen des DATENVERANTWORTLICHEN zu erbringen, wie diese in ZUSATZ 1 zu diesem ANHANG festgelegt sind und in ihrer jeweils aktuellen Fassung vom DATENVERANTWORTLICHEN kommuniziert werden. Wenn der DATENVERARBEITER der Ansicht ist, dass eine Anweisung gegen geltende DATENSCHUTZREGELUNGEN verstößt, wird er den DATENVERANTWORTLICHEN unverzüglich informieren. Der DATENVERARBEITER verpflichtet sich, die PERSONENBEZOGENEN DATEN in Übereinstimmung mit den geltenden DATENSCHUTZREGELUNGEN zu VERARBEITEN.

**3. Laufzeit und Beendigung dieses Anhangs**

**3.1.** Dieser ANHANG gilt ab dem GÜLTIGKEITSDATUM und bleibt für die Laufzeit der VEREINBARUNG in Kraft. Dieser ANHANG endet automatisch mit der Beendigung oder dem Ablauf einer LEISTUNGSBESCHREIBUNG.

**3.2.** Unbeschadet der Beendigung dieses ANHANGS sind der DATENVERARBEITER und jegliche Unterauftragnehmer weiterhin durch ihre Vertraulichkeitsverpflichtungen gebunden.

**4. Internationale Übertragungen**

Der DATENVERARBEITER ist nach den PRIVACY SHIELD Frameworks zertifiziert und hält sich an deren Prinzipien. Der DATENVERANTWORTLICHE akzeptiert, dass der DATENVERARBEITER PERSONENBEZOGENE DATEN außerhalb des EWR, dem Vereinigten Königreich und der USA VERARBEITEN kann; jedoch werden die PERSONENBEZOGENEN DATEN weiterhin in einem DATENSCHUTZLAND oder in den Vereinigten Staaten gespeichert. Der DATENVERARBEITER überträgt PERSONENBEZOGENE DATEN nur unter Einhaltung der DATENSCHUTZREGELUNGEN und benachrichtigt den DATENVERANTWORTLICHEN, wenn er kein angemessenes Schutzniveau wie durch die DATENSCHUTZREGELUNGEN gefordert mehr gewährleisten kann.

**5. Vertraulichkeit und Informationssicherheitsstandards**

**5.1.** Der DATENVERARBEITER hat PERSONENBEZOGENE DATEN streng vertraulich zu behandeln. Der DATENVERARBEITER hat sicherzustellen, dass seine Mitarbeiter sich der geltenden Datenschutz- und Informationssicherheitsanforderungen bewusst sind und durch rechtsverbindliche Vertraulichkeitsverpflichtungen gebunden sind.

**5.2.** Der DATENVERARBEITER implementiert angemessene operative, technische und organisatorische Maßnahmen zum Schutz der PERSONENBEZOGENEN DATEN gegen versehentliche oder rechtswidrige Fälle von Zerstörung, Verlust, Veränderung, unbefugter Offenlegung oder Zugang, wie in ZUSATZ 2 beschrieben.

**5.3.** Der DATENVERARBEITER aktualisiert die technischen und organisatorischen Sicherheitsmaßnahmen im Einklang mit angemessenen technologischen Entwicklungen im Ermessen des DATENVERARBEITERS und stellt dem DATENVERANTWORTLICHEN auf Anfrage eine aktualisierte Dokumentation in Form seiner aktuellen ISO-27001-Zertifizierung bereit.

**6. Kooperations- und Benachrichtigungspflichten**

**6.1.** Die PARTEIEN kooperieren miteinander, um unverzüglich und effektiv Anfragen, Reklamationen und Forderungen bezüglich der VERARBEITUNG PERSONENBEZOGENER DATEN von jeglichen Regierungsbehörden oder BETROFFENEN PERSONEN zu bearbeiten. Wenn eine BETROFFENE PERSON direkt beim DATENVERARBEITER die Ausübung ihrer Rechte in Bezug auf PERSONENBEZOGENE DATEN anfordert, hat der DATENVERARBEITER diese Anfrage unverzüglich an den DATENVERANTWORTLICHEN weiterzuleiten. Der DATENVERARBEITER hat den DATENVERANTWORTLICHEN unverzüglich zu benachrichtigen, wenn die PERSONENBEZOGENEN DATEN einer Kontrolle oder Untersuchung durch Behörden unterzogen werden, und hat keine PERSONENBEZOGENEN DATEN ohne vorige Zustimmung des DATENVERANTWORTLICHEN offenzulegen. Der DATENVERARBEITER stellt den Behörden auf Anfrage Informationen zur VERARBEITUNG im Rahmen dieses ANHANGS bereit und gestattet Inspektionen in dem in diesem ABSCHNITT 7 beschriebenen Umfang.

**6.2.** Der DATENVERARBEITER hat den DATENVERANTWORTLICHEN unverzüglich über jegliche INFORMATIONSSICHERHEITSVORFÄLLE zu benachrichtigen, welche die PERSONENBEZOGENEN DATEN beeinträchtigen. Der DATENVERARBEITER hat dem DATENVERANTWORTLICHEN die nötigen Informationen bereitzustellen und den DATENVERANTWORTLICHEN angemessen, wie durch die DATENSCHUTZREGELUNGEN gefordert, zu unterstützen.

## 7. Audit- und Inspektionsrechte des Datenverantwortlichen

Auf Anfrage des DATENVERANTWORTLICHEN hat der DATENVERARBEITER dem DATENVERANTWORTLICHEN die nötigen Informationen bereitzustellen, um die Einhaltung der Verpflichtungen im ANHANG und der DATENSCHUTZREGELUNGEN durch den DATENVERANTWORTLICHEN zu demonstrieren sowie Audits zu ermöglichen und zu unterstützen, einschließlich Inspektionen durch den DATENVERANTWORTLICHEN oder einen unabhängigen externen Prüfer, der vom DATENVERANTWORTLICHEN mit der Überprüfung der Einhaltung dieses ANHANGS durch den DATENVERANTWORTLICHEN beauftragt wurde, vorbehaltlich der Unterzeichnung einer Verschwiegenheitserklärung mit dem DATENVERARBEITER durch diese Personen. Sämtliche Inspektionen sind während der üblichen Geschäftszeiten und ohne Beeinträchtigung der Geschäftsabläufe des DATENVERARBEITERS durchzuführen.

## 8. Einsatz von Unterauftragnehmern

**8.1** Der DATENVERANTWORTLICHE erkennt hiermit an und erklärt sich damit einverstanden, dass der DATENVERARBEITER Subunternehmer zur VERARBEITUNG PERSONENBEZOGENER DATEN einsetzt. Der DATENVERARBEITER stellt dem DATENVERANTWORTLICHEN auf Anfrage sein aktuelles Subunternehmer-Verzeichnis zur Verfügung. Den jeweiligen Subunternehmern ist die VERARBEITUNG PERSONENBEZOGENER DATEN nur im Rahmen des jeweils durch den DATENVERARBEITER erteilten Auftrags gestattet, und sie sind an vertragliche Verpflichtungen gebunden, die nicht weniger schützenswert sind als dieser ANHANG. Der DATENVERARBEITER haftet für die Handlungen und Unterlassungen aller Subunternehmer im gleichen Rahmen wie für eigene Handlungen oder Unterlassungen. Der DATENVERARBEITER hält den DATENVERANTWORTLICHEN über alle Änderungen bezüglich Unteraufträgen zur DATENVERARBEITUNG auf dem Laufenden und stellt dem DATENVERANTWORTLICHEN auf Anfrage ein Exemplar dieser Unterauftragsvereinbarung zur Verfügung.

**8.2** Falls der DATENVERARBEITER beabsichtigt, einen Unterauftragnehmer zu ernennen oder zu ersetzen, der durch diesen ANHANG abgedeckt ist, hat der DATENVERARBEITER den DATENVERANTWORTLICHEN darüber im Voraus zu informieren und dem DATENVERANTWORTLICHEN die Möglichkeit einzuräumen, diesen Änderungen angemessen zu widersprechen. Der LIEFERANT hat dem DATENVERANTWORTLICHEN alle Informationen bereitzustellen, die der DATENVERANTWORTLICHE angemessenerweise verlangen könnte, um die Einhaltung der Verpflichtungen des DATENVERANTWORTLICHEN im Rahmen dieses ANHANGS und der geltenden DATENSCHUTZREGELUNGEN durch den Unterauftragnehmer zu prüfen.

## 9. Rückgabe und Löschung personenbezogener Daten

Auf Anfrage des DATENVERANTWORTLICHEN oder bei Beendigung dieses ANHANGS wird der DATENVERARBEITER alle PERSONENBEZOGENEN DATEN und Kopien davon zurückgeben oder zerstören. Auf Anfrage des DATENVERANTWORTLICHEN wird der DATENVERARBEITER bestätigen, dass er dies getan hat.

## 10. Haftung und Schadenersatz

**10.1** Die Haftung der PARTEIEN und deren Beschränkung erfolgt im Einklang mit der VEREINBARUNG.

**10.2** Der DATENVERANTWORTLICHE hat den DATENVERARBEITER gegenüber allen Forderungen von Dritten bezüglich der VERARBEITUNG PERSONENBEZOGENER DATEN schadlos zu halten, die dem DATENVERARBEITER bereitgestellt wurden, falls die VERARBEITUNG dieser Daten nicht durch die DATENSCHUTZREGELUNGEN gedeckt wurde.

| **DATENVERANTWORTLICHER:** | **DATENVERARBEITER:** |
|---|---|
| Von:_____ | Von:_____ |
| Name/Titel:_____ | Name/Titel:_____ |
| Datum:_____ | Datum:_____ |

## Zusatz 1: Verarbeitete personenbezogene Daten und Zwecke

PERSONENBEZOGENE DATEN werden zu **folgenden Zwecken übertragen und VERARBEITET**:

- Sicheres Online-Verzeichnis und Datenaustausch für Due Diligence im Unternehmen, diesbezügliche Transaktionen oder interne Geschäftszwecke.

**Verarbeitungsumfang:**

- Wie in der LEISTUNGSBESCHREIBUNG angegeben liefert der DATENVERARBEITER einen virtuellen Datenraum, ein sicheres Online-Verzeichnis zum Speichern, Verwalten, Zusammenarbeiten an und Verteilen von Daten und Dokumenten.

**Kategorien von personenbezogenen Daten:**

- Namen, Anschriften, Firmen-E-Mail-Adressen, Firmen-Telefonnummern, nationale Identifikationsnummern, Vergütung und Leistungen, Urlaubs- und Renteninformationen, Stellenbezeichnungen und -funktionen und potenziell alle anderen Arten von PERSONENBEZOGENEN DATEN, die vom Administrator des DATENVERANTWORTLICHEN in den virtuellen Datenraum hochgeladen werden.

**Besondere Datenkategorien (falls zutreffend):**

Die PERSONENBEZOGENEN DATEN betreffen die folgenden BESONDEREN DATENKATEGORIEN (bitte angeben):

- Keine, sofern nicht vom DATENVERANTWORTLICHEN anders angegeben

**Betroffene Personen:**

Die PERSONENBEZOGENEN DATEN betreffen folgende Kategorien von BETROFFENEN PERSONEN:

- Unternehmensdaten, einschließlich Daten von bzw. zu Eigentümern, Mitarbeitern, Kunden, Auftragnehmern und Lieferanten.

**Anhang 2: Maßnahmen zur Datensicherheit**

ANHANG 2 enthält:

Absatz I: Allgemeiner Datensicherheitsplan des Datenverarbeiters
Absatz II: Datensicherheitsverfahren des Datenverarbeiters

I. Allgemeiner Datensicherheitsplan

Der DATENVERARBEITER verpflichtet sich zur Einsetzung und Einhaltung der im Folgenden beschriebenen Maßnahmen zur Gewährleistung der Datensicherheit:

| | Sicherheitsanforderung | Verfahren des DATENVERARBEITERS zur Umsetzung der jeweiligen Datensicherheitsmaßnahme |
|---|---|---|
| | Bitte beschreiben Sie die Maßnahmen zur (physischen) Zugangskontrolle, mit denen in Ihrem Unternehmen verhindert wird, dass sich unbefugte Personen Zugang zu Systemen verschaffen, in denen PERSONENBEZOGENE DATEN VERARBEITET oder verwertet werden (bei Unternehmen mit mehreren Tochtergesellschaften oder | Alle Rechenzentren sind gemä´ß ISO 27001:2013 und SOC 2 Typ 2 zertifiziert. Zudem sind die Rechenzentren gemäß den PRIVACY SHIELD Frameworks zertifiziert.<br><br>Der Zugang zu allen Rechenzentren ist durch mehrere Sicherheitskontrollen gesichert, die eine mehrfache Authentifizierung anhand unterschiedlicher Methoden erfordern. |
| 2. | Bitte beschreiben Sie die Maßnahmen zur Zugangskontrolle, mit denen in Ihrem Unternehmen der unbefugte Zugriff auf Datenverarbeitungssysteme verhindert wird. | Zugriffsbefugnis ist an Geschäftserfordernisse gebunden und erfordert Rollenidentifizierung und -genehmigung seitens der Geschäftsführung. Zeitsperren, starke Authentifizierungsanforderungen und Zugriffsberechtigungen werden nachverfolgbar eingesetzt. |
| 3. | Bitte beschreiben Sie die Maßnahmen zur (virtuellen) Zugangskontrolle, mit denen in Ihrem Unternehmen gewährleistet wird, dass Personen, die zur Nutzung eines Verarbeitungssystems berechtigt sind, ausschließlich im Rahmen ihrer jeweiligen Berechtigung auf PERSONENBEZOGENE DATEN zugreifen können und dass | Der Anwenderzugriff wird über ein förmliches Verfahren zur An- und Abmeldung verwaltet, wobei der Zugriff auf sämtliche Systeme und DIENSTE auf Rollenbasis gewährt und widerrufen wird. Durch Revisionsberichterstattung wird eine präzise Überwachung von Anwenderaktivitäten gewährleistet; zusätzlich werden Zugangskontrollen zum Schutz der Integrität und Vertraulichkeit der Daten eingesetzt. |
| 4. | Beschreiben Sie die Maßnahmen zur Übertragungskontrolle, mit denen in Ihrem Unternehmen gewährleistet wird, dass PERSONENBEZOGENE DATEN während der elektronischen Übertragung oder Weiterleitung nicht ohne Bevollmächtigung gelesen, kopiert, geändert oder gelöscht werden können und dass überprüft und festgestellt werden kann an welche | Der DATENVERARBEITER wendet eine Richtlinie für Wechselmedien mit entsprechenden technischen Kontrollen an, um die Integrität und Vertraulichkeit der Daten zu schützen und die unbefugte Übertragung PERSONENBEZOGENER DATEN zu verhindern. Der serverferne Zugriff wird über Multifaktor-Authentifizierung gesteuert. Daten werden im Ruhezustand und während der Übertragung mit staatlich anerkannten Verschlüsselungstechnologien verschlüsselt. |

| | | |
|---|---|---|
| 5. | Beschreiben Sie die Maßnahmen zur Eingabekontrolle, mit denen gewährleistet wird, dass überprüft und festgestellt werden kann, ob und von wem PERSONENBEZOGENE DATEN in Verarbeitungssysteme eingegeben, geändert oder gelöscht | Der DATENVERARBEITER verhält sich neutral zu den vom Kunden hochgeladenen Daten. Sämtliche Anwenderaktivitäten in Bezug auf die Integrität und Vertraulichkeit der Daten werden nachverfolgt und sind berichtspflichtig. Die Entscheidung, welche Daten dem DATENVERARBEITER bereitgestellt werden, liegt im alleinigen Ermessen des |
| 6. | Beschreiben Sie die Maßnahmen zur Zuordnungskontrolle, mit denen in Ihrem Unternehmen gewährleistet wird, dass die auftragsgemäße VERARBEITUNG von PERSONENBEZOGENEN DATEN unter strikter Einhaltung der | Im Rahmen der Zertifizierung gemäß ISO 27001 und der Berichtspflicht nach SOC 2 Typ 2 werden jährlich Revisionsverfahren zur Gewährleistung der Konformität mit allen gültigen Vorschriften durchgeführt. Befugte Anwender schließen eine entsprechende Schulung ab und bescheinigen jährlich die Konformität mit dem Verhaltenskodex und den Richtlinien des Unternehmens. |
| 7. | Beschreiben Sie die Maßnahmen zur Verfügbarkeitskontrolle, mit denen in Ihrem Unternehmen gewährleistet wird, dass PERSONENBEZOGENE DATEN vor versehentlicher Zerstörung oder Verlust geschützt sind. | Der DATENVERARBEITER sichert alle Plattformen durch Redundanz und führt Protokolle zur Systemverfügbarkeit. Zusätzlich werden durch Redundanz laufende Backup-Sicherungen des Systems ermöglicht.<br><br>Der DATENVERARBEITER verfügt über Pläne zur Notfallwiederherstellung und Betriebskontinuität, die |
| 8. | Beschreiben Sie die Maßnahmen zur Trennungskontrolle, mit denen in Ihrem Unternehmen die getrennte VERARBEITUNG PERSONENBEZOGENER DATEN gewährleistet wird, die zu | Innerhalb einer mandantenfähigen Datenbank wird eine logische Trennung aufrechterhalten. Der befugte Zugriff beschränkt sich entsprechend der jeweiligen Bevollmächtigung des Anwenders auf spezifische Projekte. Der DATENVERARBEITER setzt eine dreistufige Anwendung mit Datentrennung zwischen |

II. Datensicherheitsverfahren des Datenverarbeiters

Der DATENVERARBEITER verpflichtet sich zur Umsetzung und Einhaltung der im Folgenden beschriebenen Normen, Abläufe und Verfahren:

Datasite betreibt ein Managementsystem für Datensicherheit, das die Anforderungen der ISO/IEC 27001: 2013 im folgenden Rahmen erfüllt: Die Verwaltung der Datensicherheit umfasst Verfahren zum Schutz von Kundendaten im Rahmen globaler DIENSTE im Bereich Finanztransaktionen und -berichterstattung, Marketing und Kommunikation für regulierte Branchen sowie Kundeninhalte und Kooperationen.