Hotel Beacons Saas-Vertrag – Auftragsverarbeitungsvereinbarung (Anlage 3 zum Angebot)

Vereinbarung zwischen dem Vertragspartner („**Auftraggeber**“) und der Hotel Beacons GmbH („**Auftragnehmer**“) über die Verarbeitung von personenbezogenen Daten im Auftrag („**Vereinbarung**“). Definitionen in den AGB oder der Leistungsbeschreibung gelten auch in dieser Auftragsverarbeitungsvereinbarung. Definitionen in dieser Auftragsverarbeitungsvereinbarung gelten nur für diese Auftragsverarbeitungsvereinbarung.

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer entsprechend der Leistungsbeschreibung in Anlage 2 zum Angebot: Hotel Services, Targeting Services, Betrieb des Conichi Merchant Centers, Targeting Services, Betrieb der Whitelabel App und Whitelabel Website, die Corporate Travel Services sowie ggf. sonstige Services, wie in Anlage 2 zum Angebot beschrieben. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage der AGB.

1.2. Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Vertrages.

2. Konkretisierung des Auftragsinhalts

2.1. Umfang, Art und Zweck

Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsbeschreibung in Anlage 2 zum Angebot.

2.2. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien

- Gastdaten (z.B. Name, Kontaktdaten, Präferenzen),
- Gast-Besuchsdaten,
- Targeting-Daten,
- Hotelinformationen,
- Mitarbeiterdaten, und
- Sonstige Daten, die vom Auftragnehmer oder dessen Mitarbeitern oder Kunden in die Merchant-App, das Conichi Merchant Center, die Whitelabel App oder die Whitelabel Website geladen werden.

Es wird klargestellt, dass der Auftragnehmer selbst verantwortliche Stelle für einige dieser Datenkategorien ist, wenn und soweit er diese für eigene Zwecke verarbeitet (z.B. Gastdaten zum Betrieb des Gast-Accounts bei conichi).

2.3. Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

□ Hotelgäste,

□ Interessenten

□ Beschäftigte, sowie

□ Geschäftskontakte

3. Weisungsbefugnis des Auftraggebers / Ort der Datenverarbeitung

3.1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers (vgl. Art. 28 Abs. 3 lit. a DSGVO). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Entstehende Zusatzaufwände sind vom Auftraggeber auf Time- und Material-Basis zu vergüten. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

3.2. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Soweit der Auftragnehmer als Auftragsdatenverarbeiter agiert, verwendet dieser die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Verpflichtungen nach Unionsrecht oder dem Recht eines EU-Mitgliedstaats, sowie zur Einhaltung von Aufbewahrungspflichten erforderlich sind.

3.3. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend Art. 28 Abs. 3 Uabs. 2 DSGVO zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

3.4. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer findet innerhalb der EU / des EWR statt. Der Auftragnehmer ist verpflichtet, den Auftraggeber vor Aufnahme der Verarbeitung auf eine gesetzliche Verpflichtung des Auftragnehmers hinzuweisen, die Verarbeitung der Auftraggeberdaten an einem anderen Ort durchzuführen, sofern eine solche Mitteilung nicht gesetzlich untersagt ist. Die Verarbeitung und / oder Verbringung in ein Drittland außerhalb des Gebietes der EU / EWR oder an eine internationale Organisation bedarf der vorherigen schriftlichen Zustimmung des

Auftraggebers. In diesem Fall ist der Auftragnehmer zudem verpflichtet, entsprechend den gesetzlich anwendbaren Vorgaben sowie gerichtlichen und behördlichen Auslegungen derselben für ein angemessenes Datenschutzniveau am Ort der Datenverarbeitung zu sorgen oder – nach Wahl des Auftraggebers – dem Auftraggeber die Möglichkeit einzuräumen, für ein angemessenen Datenschutzniveau zu sorgen, unter anderem durch den Abschluss von oder dem Beitritt zu EU-Standardvertragsklauseln.

4. Vertraulichkeit

Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung von personenbezogenen Daten befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- / Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Technisch-organisatorische Maßnahmen

5.1. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird angemessene technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DSGVO genügen. Insbesondere sind die technischen und organisatorischen Maßnahmen dergestalt zu treffen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sichergestellt sind. Diese technischen und organisatorischen Maßnahmen sind in Anhang 1 dieser Vereinbarung beschrieben. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

5.2. 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.

6. Unterauftragsverhältnisse

6.1. Die Einschaltung und/oder Änderung von Unterauftragnehmern durch den Auftragnehmer ist grundsätzlich nur mit Zustimmung des Auftraggebers gestattet. Der Auftraggeber stimmt dem Einsatz von Unterauftragnehmern wie folgt zu:

6.1.1. Der Auftraggeber stimmt dem Einsatz der in Anhang 2 dieser Vereinbarung aufgeführten Unterauftragnehmer bereits jetzt zu.

6.1.2. Der Auftraggeber stimmt dem Einsatz bzw. der Änderung weiterer Unterauftragnehmer zu, wenn der Auftragnehmer den Einsatz bzw. die Änderung dreißig (30) Tage vor Beginn der Datenverarbeitung schriftlich (E-Mail ausreichend) dem Auftraggeber mitteilt. Der Auftraggeber kann dem Einsatz eines neuen Unterauftragnehmers bzw. der Änderung widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zum Einsatz oder zur Änderung als gegeben. Der Auftraggeber nimmt zur Kenntnis, dass in bestimmten Fällen die Leistung ohne den Einsatz eines bestimmten Unterauftragnehmers nicht mehr erbracht werden kann. In diesen Fällen ist jede Partei zur Kündigung ohne die Einhaltung einer Frist berechtigt. Liegt ein wichtiger datenschutzrechtlicher Grund für den Widerspruch vor und ist eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

6.2. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie dieselben Datenschutzpflichten wie in diesem Auftrag vereinbart enthalten, unter Berücksichtigung der Art und des Umfangs der Datenverarbeitung im Rahmen des Unterauftrags. Die Verpflichtung des Unterauftragsverarbeiters muss schriftlich erfolgen bzw. im elektronischen Format.

6.3. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7. Betroffenenrechte

7.1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen nach Kapitel III der DSGVO.

7.2. Der Auftragnehmer hat nur nach Weisung des Auftraggebers über die Daten, die im Auftrag verarbeitet werden, Auskunft zu geben, diese Daten zu berichtigen, zu löschen oder die Datenverarbeitung entsprechend einzuschränken. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung oder Löschung seiner / ihrer Daten sowie hinsichtlich der Einschränkung der Datenverarbeitung wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

8. Mitwirkungspflichten des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.

8.2. Im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO gilt Folgendes: Der Auftragnehmer ist verpflichtet, den Auftraggeber (i) über die Verletzung des Schutzes personenbezogener Daten unverzüglich zu informieren und (ii) bei einer solchen Verletzung erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO (Meldungen und Benachrichtigungen bei Verletzung des Schutzes personenbezogener Daten) für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziffer 3 dieser Vereinbarung durchführen.

8.3. Soweit der Auftraggeber im Falle eines Sicherheitsvorfalles Benachrichtigungs- oder Mitteilungspflichten hat, verpflichtet sich der Auftragnehmer, den Auftraggeber auf dessen Kosten zu unterstützen.

9. Sonstige Pflichten des Auftragnehmers

9.1. Soweit gesetzlich vorgeschrieben bestellt der Auftragnehmer einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO, §§ 38, 6 BDSG neu ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme auf Anfrage mitgeteilt.

9.2. Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO unterrichten. Dies gilt auch, soweit eine zuständige Behörde nach Art. 83 DSGVO beim Auftragnehmer ermittelt.

9.3. Der Auftragnehmer wir die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. –erfüllung sicherstellen, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

10. Informations- und Überprüfungsrecht des Auftraggebers

10.1. Der Auftraggeber hat das Recht, die nach Art. 28 Abs. 3 h) DSGVO erforderlichen Informationen zum Nachweis der Einhaltung der vereinbarten Pflichten des Auftragnehmers anzufordern und Überprüfungen im Einvernehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

10.2. Die Parteien vereinbaren, dass der Auftragnehmer zum Nachweis der Einhaltung seiner Pflichten und Umsetzung der technischen und organisatorischen Maßnahmen berechtigt ist, dem Auftraggeber aussagekräftige Dokumentationen vorzulegen. Eine aussagekräftige Dokumentation kann durch die Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter), einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001) oder einer durch die zuständigen Aufsichtsbehörden genehmigten Zertifizierung erbracht werden.

10.3. Das Recht des Auftraggebers Vor-Ort-Kontrollen durchzuführen, wird hierdurch nicht beeinträchtigt. Der Auftraggeber wird jedoch abwägen, ob nach Vorlage von aussagekräftiger Dokumentation eine Vor-Ort-Kontrolle noch erforderlich ist, insbesondere unter Berücksichtigung der Aufrechterhaltung des ordnungsgemäßen Betriebs des Auftragnehmers.

10.4. Der Auftraggeber 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. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

11. Löschung von Daten und Rückgabe von Datenträgern

Nach Wahl und Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Vertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Haftung

Die Haftung der Parteien aus dieser Vereinbarung richtet sich nach den Haftungsregelungen in Ziffer 9 der AGB.

Anhang 1 zur Auftragsverarbeitungsvereinbarung:

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO.

Der Auftragnehmer hat die folgenden technischen und organisatorischen Sicherheitsmaßnahmen implementiert, um die laufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und -dienste zu gewährleisten:

1. Vertraulichkeit

Der Auftragnehmer hat folgende technische und organisatorische Sicherheitsvorkehrungen getroffen, um insbesondere die Vertraulichkeit der Verarbeitungssysteme und -dienste zu gewährleisten:

- Der Auftragnehmer verarbeitet alle Kundendaten an europäischen Serverstandorten, die von branchenführenden Cloud Service Providern betrieben werden, die hochentwickelte Maßnahmen zum Schutz vor unbefugtem Zugriff auf Datenverarbeitungsanlagen (insbesondere Telefone, Datenbank- und Applikationsserver und zugehörige Hardware) anbieten.
  Zu diesen Maßnahmen gehören:
  - ein mehrschichtiges Sicherheitsmodell, das Sicherheitsvorkehrungen wie maßgeschneiderte elektronische Zugangskarten, Alarme, Fahrzeugzutrittsschranken, Umzäunungen, Metalldetektoren und Biometrie umfasst, sowie eine Ausstattung des Bodens des Rechenzentrums mit einer Laserstrahleinbruchhemmung;
  - Rechenzentren werden rund um die Uhr von hochauflösenden Innen- und Außenkameras überwacht, die unberechtigte Personen erkennen und verfolgen können;
  - Zugriffsprotokolle, Aktivitätsaufzeichnungen und Kameraaufnahmen sind für den Fall eines Einbruchs verfügbar;
  - Rechenzentren werden außerdem routinemäßig von erfahrenen Sicherheitskräften patrouilliert, die strenge Hintergrundüberprüfungen und Schulungen durchlaufen haben;
  - Der Zugang zum Boden des Rechenzentrums ist nur über einen Sicherheitskorridor möglich, der eine mehrstufige Zugangskontrolle mittels Sicherheitsausweisen und Biometrie ermöglicht;
  - Nur berechtigte Mitarbeiter mit bestimmten Rollen können eintreten.
- Der Auftragnehmer trifft geeignete Maßnahmen, um zu verhindern, dass seine Datenverarbeitungssysteme von Unbefugten benutzt werden. Dies wird erreicht durch:
  - automatisches Timeout des User-Terminals, wenn dieser im Leerlauf bleibt, Identifikation und Passwort zum erneuten Zugreifens erforderlich;
  - Ausgabe und Sicherung von Identifikationscodes an die Online-Plattform des Auftragnehmers, die eine Zwei-Faktor-Authentifizierung für alle Benutzer erfordert;
  - Kunden können individuelle Benutzerkonten mit Berechtigungen für alle Auftragnehmer-Ressourcen definieren;
  - Verschlüsselung nach Industriestandard und Anforderungen an Passwörter (Mindestlänge, Verwendung von Sonderzeichen usw.); und
  - Alle Zugriffe auf Dateninhalte werden protokolliert, überwacht und verfolgt.
- Die Mitarbeiter des Auftragnehmers, die zur Nutzung seiner Datenverarbeitungssysteme berechtigt sind, können nur im Rahmen und in dem Umfang auf personenbezogene Daten zugreifen, der durch ihre jeweilige Zugriffsberechtigung (Berechtigung) abgedeckt ist. Insbesondere basieren die Zugriffsrechte und -ebenen auf der Funktion und Rolle der Mitarbeiter, wobei die Konzepte der geringsten Privilegien und des Wissensbedarfs verwendet werden, um die Zugriffsrechte an definierte Verantwortlichkeiten anzupassen. Dies wird erreicht durch:
  - Mitarbeiterpolitik und -schulung;
  - wirksame und angemessene Disziplinarmaßnahmen gegen Personen, die unbefugt auf personenbezogene Daten zugreifen;
  - beschränkter Zugriff auf personenbezogene Daten nur für autorisierte Personen;
  - Verschlüsselung nach Industriestandard und
  - Richtlinien zur Kontrolle der Aufbewahrung von Sicherungskopien.

2. Integrität

Der Auftragnehmer hat die folgende technische und organisatorische Sicherheit implementiert, um insbesondere die Integrität der Verarbeitungssysteme und -dienste zu gewährleisten:

- Der Verarbeiter trifft geeignete Maßnahmen, um zu verhindern, dass personenbezogene Daten bei der Übermittlung oder beim

Transport der Datenträger von Unbefugten gelesen, kopiert, verändert oder gelöscht werden. Dies wird erreicht durch:

- Den Einsatz modernster Firewall- und Verschlüsselungstechnologien zum Schutz der Torwege und Pipelines, durch die die Daten fließen;
- Verschlüsselung nach Industriestandard und
- Vermeidung der Speicherung personenbezogener Daten auf tragbaren Speichermedien für Transportzwecke und auf firmeneigenen Laptops oder anderen mobilen Geräten.

- Der Auftragnehmer greift auf keine Kundeninhalte zu, es sei denn, dies ist notwendig, um dem Kunden die von ihm ausgewählten Produkte und professionelle Dienstleistungen zur Verfügung zu stellen. Der Auftragnehmer greift nicht auf Kundeninhalte für andere Zwecke zu. Entsprechend weiß der Auftragnehmer nicht, welche Inhalte Kunden auf seinen Systemen speichern und kann nicht zwischen persönlichen Daten und anderen Inhalten unterscheiden, so dass der Auftragnehmer alle Kundeninhalte gleich behandelt. Auf diese Weise profitieren alle Kundeninhalte von den gleichen hohen Sicherheitsmaßnahmen des Auftragnehmers, unabhängig davon, ob diese Inhalte personenbezogene Daten enthalten oder nicht.

3. Verfügbarkeit

- Der Auftragnehmer hat die folgenden technischen und organisatorischen Sicherheitsmaßnahmen implementiert, um insbesondere die Verfügbarkeit von Verarbeitungssystemen und -diensten zu gewährleisten:
  - Der Verarbeiter trifft geeignete Maßnahmen, um sicherzustellen, dass personenbezogene Daten vor unbeabsichtigter Zerstörung oder Verlust geschützt sind. Dies wird erreicht durch:
  - Redundanz der Infrastruktur;
  - Richtlinien, die eine permanente lokale (Arbeitsplatz) Speicherung personenbezogener Daten verbieten; und
  - Durchführung regelmäßiger Datensicherungen.

4. Belastbarkeit

- Der Auftragnehmer hat die folgenden technischen und organisatorischen Sicherheitsmaßnahmen implementiert, um insbesondere die Ausfallsicherheit der Verarbeitungssysteme und -dienste zu gewährleisten:

Anhang 2 zur Auftragsverarbeitungsvereinbarung

Genehmigte Unterauftragnehmer

#	Name	Adresse	Einsatzbereich im Rahmen des Vertrages
1			*[z.B. Hosting und Betrieb der Plattform ODER Softwareentwicklung, Softwarepflege]*
2			