Auftrag zur Datenverarbeitung gemäß DSGVO

Information und Ausfüllhilfe

1. Bitte füllen Sie alle fehlenden Angaben in der nachfolgenden Vereinbarung zum Datenschutz aus:

- **Seite 1**: Firmenanschrift
- **Seite 12**: Ort, Datum, Funktion und Unterschrift
- **Seite 14**: Ansprechpartner

2. Drucken Sie die ausgefüllte Vereinbarung zweimal aus und lassen Sie beide Exemplare von der zeichnungsbefugten Person unterzeichnen.

3. Schicken Sie uns die Vereinbarung in zweifacher, unterschriebener Ausführung zu.

4. Sobald wir die Vereinbarung erhalten und geprüft haben, schicken wir Ihnen zeitnah ein gegengezeichnetes Exemplar zurück.

Datenverarbeitung im Auftrag

Vereinbarung gemäß Art. 28 DSGVO

zwischen:

Firmenname:

Anschrift:

- nachstehend „Auftraggeber“ genannt -

und

Astrotel Internetmarketing GmbH

Leipziger Str. 1

15566 Schöneiche

- nachstehend "Auftragnehmer" genannt -.

für Hosting Services und Online-Buchungssysteme

1 Gegenstand und Dauer des Auftrags

Vereinbarungsgegenstand ist die Auftragsverarbeitung im Sinne Art. 28 EU Datenschutz-Grundverordnung (DSGVO). Im Detail handelt es sich um alle notwendigen und vereinbarten Maßnahmen zur Programmierung, Bereitstellung sowie Pflege und Wartung eines onlinebasierten Buchungssystems für Unterkünfte, über das der Auftraggeber verschiedene Leistungen und Produkte (Objekte) verwaltet, online gebucht und abgerechnet werden können, Webseiten und Bereitstellung von Email-Konten.
Im Zuge der Bereitstellung des Systems sowie bei Programmierungs-, Wartungs- und Pflegearbeiten können dem Auftragnehmer Kunden- und Interessentendaten des Auftraggebers bekannt werden.
Die Einzelheiten der Leistungen ergeben sich aus den Allgemeinen Geschäftsbedingungen (https://www.astrotel.net/uploads/20160226092117.pdf), die bei der Registrierung ausdrücklich vom Auftraggeber akzeptiert werden. Auf diese Leistungen wird hier verwiesen (im Folgenden Nutzungsbedingungen).
Der Vertrag regelt die datenschutzrechtlichen Maßnahmen im Sinne von Art. 28 DSGVO und die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der datenschutzrechtlichen Anforderungen.
Der Vertrag wird auf unbestimmte Zeit geschlossen. Die Regelungen zur Kündigung der Nutzungsbedingungen gelten auch für diesen Vertrag. Die Geheimhaltungspflichten des Auftragnehmers bleiben auch über das Vertragsende hinaus bestehen.

2 Datenarten/-kategorien

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

- Kontaktdaten und –historie bzgl. natürlicher Personen d.h. Kunden, Lieferanten, Mitarbeiter, Leiharbeitskräfte, Ansprechpartner von Firmen, Interessenten und Vertretern
- Daten zur Geschäftshistorie von Kunden, Lieferanten und Vertretern
- Daten von Mitarbeitern, Leiharbeitskräften bzw. Anwendern des Systems
- Daten zu finanziellen Transaktionen von Kunden, Lieferanten, Mitarbeitern und Vertretern
- Daten zu Bankverbindungen und Zahlungsarten von Kunden, Lieferanten und Vertretern
- Sonstige (unstrukturierte) personenbezogenen Daten von Kunden, Lieferanten, Ansprechpartnern von Firmen, Interessenten, Vertretern, Mitarbeitern, Leiharbeitskräfte und Anwendern des Systems

Die übertragenen personenbezogenen Daten betreffen die folgenden Personengruppen:

- Kunden
- Lieferanten
- Ansprechpartner

3 Ort der Verarbeitung

Die Datenverarbeitung findet auf dem Gebiet der Bundesrepublik Deutschland oder innerhalb der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes statt. Das Hosting der Software Services für die überlassenen Daten erfolgt auf Webservern in Deutschland. Das Rechenzentrum wird betrieben von Vautron Rechenzentrum AG. Der Auftragnehmer hat eine Standarddatenschutzklausel (Art. 46 Abs. 2 litt. c und d DSGVO) mit dem Hoster abgeschlossen.

Eine Verarbeitung in anderen Staaten ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Der Auftragnehmer führt den Nachweis für das Bestehen der Garantien und eines angemessenen Schutzniveaus. Der Nachweis kann durch Vorlage eines entsprechenden Zertifikates einer akkreditierten Zertifizierungsstelle nach Art. 43 DSGVO geführt werden. Der Auftragnehmer verpflichtet sich, die Einhaltung der Garantien und eines angemessenen Schutzniveaus sicherzustellen.

4 Zweckbindung

Personenbezogene Daten, die dem Auftragnehmer im Rahmen der Erfüllung des Gesamtvertrages bekannt werden, darf dieser nur zur Erfüllung der beauftragten Tätigkeiten im unbedingt notwendigen Umfang verwenden. Der Auftragnehmer verpflichtet sich, erhaltene Daten unter keinen Umständen unbefugt zu verarbeiten, zu verändern oder anderweitig zu nutzen. Eine Weitergabe dieser Daten an „Dritte“ i.S.d. DSGVO findet nicht statt.
Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es zur Erfüllung der Aufgabe notwendig ist. Dem Auftragnehmer ist es insbesondere untersagt, Daten die dieser Vereinbarung unterfallen, für eigene Geschäftszwecke zu verwenden, für andere Auftraggeber zu nutzen und die Speicherung der Daten nach Auftragsabwicklung fortzusetzen.

5 Weisungsbefugnisse des Auftraggebers

Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über Art, Umfang und Verfahren der Datenverarbeitung sowie über Änderungen der Verarbeitung vor. Die Weisungen betreffen insbesondere aber nicht ausschließlich die datenschutzkonforme Auftragsabwicklung und sonstige Handlungen zur Sicherstellung einer gesetzmäßigen Auftragsabwicklung. Die Weisungen werden schriftlich, in Schriftform oder in einem anderen geeigneten elektronischen Format erteilt. Mündliche Weisungen werden unverzüglich in Schriftform, schriftlich oder in einem elektronischen Format bestätigt. Die Weisungen werden über die Dauer des Auftragsverhältnisses, mindestens jedoch für die Dauer ihrer Gültigkeit aufbewahrt.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften verstößt. Der Auftragnehmer kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Der Auftraggeber haftet für rechtswidrige Weisungen und stellt den Auftragnehmer insoweit von Schadensersatzansprüchen und sonstigen Forderungen frei.
Weisungsberechtigte Personen des Auftraggebers und des Auftragnehmers sind in Anlage 2 dieser Vereinbarung aufzuführen. Änderungen der weisungsberechtigten Person oder Weisungsempfänger sind unverzüglich mitzuteilen.

6 Pflichten des Auftraggebers

Für die Richtigkeit und für die Zulässigkeit der Datenerhebung und -nutzung sowie für die Wahrung der Rechte der Betroffenen i.S.d. DSGVO ist und bleibt der Auftraggeber verantwortlich.
Der Auftraggeber ist „verantwortliche Stelle“ i.S.d. DSGVO für die Erhebung, Verarbeitung und/oder Nutzung der personenbezogenen Daten.
Der Auftraggeber ist als verantwortliche Stelle für die Wahrung der Betroffenenrechte nach Artt. 12 bis 23 DSGVO verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen.
Der Auftraggeber hat die Nutzer seiner Website in einer Datenschutzerklärung über die Verarbeitung und Übermittlung personenbezogener Daten im Rahmen der Onlinebuchung und Nutzung zusätzlicher Dienste des Auftragnehmers aufzuklären und auf die Widerspruchsmöglichkeiten hinweisen.
Die Pflicht zur Führung des Verzeichnisses für Verarbeitungstätigkeiten nach Art. 30 DSGVO liegt beim Auftraggeber.
Die Pflicht zur Durchführung der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO liegt beim Auftraggeber.
Dem Auftraggeber obliegen die Informationspflichten nach Artt. 33, 34 DSGVO.
Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragserteilung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
Nach Beendigung der Datenverarbeitung im Auftrag legt der Auftraggeber die Maßnahmen zur Rückgabe der überlassenen Daten und Datenträger und/oder Löschung gespeicherter Daten durch Weisung fest.
Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherungsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

7 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, (Fern-) Wartungsarbeiten mit Zugriff auf personenbezogene Daten nur auf Weisung des Auftraggebers von hierzu autorisierten und benannten Mitarbeitern durchführen zu lassen.
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.
Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Als Ansprechpartner beim Auftragnehmer wird DSBextern.de Stefan Spörrer Hofbauerstraße 3a 94209 Regen

Tel: 09921-807780 E-Mail: stefan.spoerrer@dsbextern.de benannt.
Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.
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.
Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Auftraggebers nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrages oder zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich ist oder eine gesetzliche oder sonstige Aufbewahrungspflicht besteht. Eventuell hergestellte Auszüge, Kopien oder Duplikate sind nach Abschluss der Verarbeitung oder Nutzung vom Auftragnehmer unverzüglich sicher zu löschen bzw. datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen.

Duldungspflichten bei Kontrollen

Der Auftragnehmer verpflichtet sich, in Prüfungen durch den Auftraggeber die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nachzuweisen, Auskünfte zu erteilen und die entsprechenden Unterlagen vorzulegen bzw. Einsicht in die erforderlichen Unterlagen und Systeme zu gewähren und nach vorheriger Abstimmung entsprechende Prüfungen des Auftraggebers vor Ort zu dulden und zu unterstützen. Er verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.
Der Nachweis angemessener technischer und organisatorischer Maßnahmen kann auch durch Vorlage von Testaten oder Zertifikaten oder durch eine Zertifizierung bzw. ein Datenschutzaudit einer unabhängigen Einrichtung bzw. eines autorisierten Sachverständigen geführt werden. Unabhängig von diesen Nachweisen ist der Auftragnehmer verpflichtet, Kontrollen durch den Auftraggeber dieser Vereinbarung zu dulden.

Informationspflichten

Der Auftragnehmer ist verpflichtet, wesentliche Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmäßigkeit der

Durchführung der Auftragsleistungen herabsetzen, unaufgefordert dem Auftraggeber zu melden.
Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen der Aufsichtsbehörde für den Datenschutz, insbesondere gem. Art. 58 DSGVO, und über eventuelle Maßnahmen und Auflagen zum Schutz der personenbezogenen Daten.
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.
Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten und Änderungen in der Person des betrieblichen Datenschutzbeauftragten oder, wenn keine Bestellpflicht besteht, den Namen und die Kontaktdaten der sonstigen zuständigen Stelle mit.

Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. e und f DSGVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutz-Folgeabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutz-Folgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

Organisationspflichten

Der Auftragnehmer verpflichtet sich zur Einrichtung von Maßnahmen und Dokumentationen, die eine Kontrolle und Nachvollziehbarkeit aller mit der Auftragsverarbeitung zusammenhängenden Tätigkeiten und Verarbeitungsprozesse im Sinne einer Auftragskontrolle und der Ordnungsmäßigkeit der Datenverarbeitung ermöglichen. Datenschutzvorfälle und sonstige sicherheitsrelevante Störungen der Verarbeitung sind einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren und dem Auftraggeber zu melden. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.
Wird die Verarbeitung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, ist der Auftraggeber darüber zu informieren. Der Auftragnehmer verpflichtet sich, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Verarbeitung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung vom Ort des Auftragnehmers aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.

8 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

Personenbezogene und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der personenbezogenen Daten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrages bekannt werdenden

personenbezogenen Daten und sonstige unternehmensinterne Umstände, Daten und Informationen (Betriebsgeheimnisse) vertraulich zu behandeln sowie die im Rahmen dieses Vertrages tätig werdenden Mitarbeiter auch über die Beendigung des Beschäftigungsverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Verarbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.
Der Auftragnehmer verpflichtet sich zur Beachtung aller sonstigen Geheimnisse, soweit diese für die Verarbeitung einschlägig sind, wie des Sozialgeheimnisses, des Fernmeldegeheimnisses und sonstiger Berufsgeheimnisse gem. § 203 StGB sowie zur Verpflichtung und Belehrung der Beschäftigten zur Sicherstellung der Wahrung dieser Geheimnisse.
Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über administrative Zugangsdaten und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen. Von den ihm eingeräumten Zugriffsrechten darf der Auftragnehmer nur in dem Umfang Gebrauch machen, der für die Durchführung der Datenverarbeitung erforderlich ist. Die Verpflichtung zur Wahrung der Vertraulichkeit und der sonstigen Geheimnisse gilt auch über die Beendigung dieses Vertrages hinaus.

9 Unterauftragsverhältnisse

Die Einschaltung von Unterauftragnehmern ist nur zulässig, wenn der Auftragnehmer vor der Vergabe der Auftragsleistung den Auftraggeber schriftlich informiert und der Auftraggeber nicht widersprochen hat. Anlage 1 enthält eine aktuelle Übersicht zu den Unterauftragnehmern.
Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes, insbesondere bei einer Gesetzes- oder Vertragsverletzung, seine Zustimmung zur Unterbeauftragung widerrufen. Unterbeauftragung ist dann unverzüglich einzustellen. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen dieses Vertrages entsprechen. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterverarbeitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn ein Vertrag nach diesen Auflagen abgeschlossen worden ist und der Unterauftragnehmer alle Anforderungen dieses Vertrages erfüllt hat.
Bei der Unterbeauftragung sind dem Unterauftragnehmer die gleichen vertraglichen Regelungen aufzuerlegen, wie sie für den Auftragnehmer gelten. Dem Auftraggeber sind gegenüber dem Unterauftragnehmer die gleichen Weisungs-, Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und dem Art. 28 DSGVO einzuräumen, wie sie gegenüber dem Auftragnehmer gelten. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

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 fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
Eine Beauftragung von Unterauftragnehmern außerhalb des Gebiets der Bundesrepublik Deutschland oder der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Im Übrigen gelten die Regelungen zu Nr. 3 dieser Vereinbarung auch für die Beauftragung von Unterauftragnehmern.

10 Mitteilungspflichten bei Störungen und Datenschutzverletzungen

Bei einer Störung der Verarbeitung oder einer Datenschutzverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und für den Auftraggeber ein.
Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der personenbezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können. Zu den Datenschutzverstößen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne dieses Vertrages.
Die Meldung an den Auftraggeber umfasst alle Informationen, die für den Auftraggeber erforderlich sind, um den Vorfall und seine Meldepflicht an die Aufsichtsbehörde und die Informationspflicht der Betroffenen gem. Art. 33 und 34 DSGVO beurteilen und ggf. fristgerecht die Meldung an die Aufsichtsbehörde und ggf. die Information der Betroffenen vornehmen zu können. Die Meldung an den Auftraggeber umfasst insbesondere Angaben zur Art des Vorfalls und der Verletzung des Schutzes von personenbezogenen Daten, eine Beschreibung der wahrscheinlichen Risiken für die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen und eine Beschreibung der bereits eingeleiteten Maßnahmen zur Behebung bzw. Reduzierung eines möglichen Schadens oder sonstiger Risiken für die Betroffenen und den Auftraggeber.
Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 33 und 34 DSGVO und unternimmt alle in seinen Verantwortungsbereich fallenden Maßnahmen zur Minderung

nachteiliger Folgen für die Betroffenen sowie zur Aufklärung des Vorfalls und dessen Folgen. Dies gilt auch nach Beendigung des Vertragsverhältnisses.

11 Rechte der Betroffenen

Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zuständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen.
Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarten Kontaktpersonen erteilt werden.

12 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, 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.
Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

13 Technische und organisatorische Maßnahmen

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. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der 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 DSGVO zu berücksichtigen [Einzelheiten in Anlage 3 & 4].

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.

14 Verfahren nach Beendigung des Auftrages

Nach Abschluss der Verarbeitung, spätestens nach Beendigung dieses Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten personenbezogenen oder sonstige vertrauliche Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder in Abstimmung mit dem Auftraggeber datenschutzgerecht zu vernichten oder sicher zu löschen. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen. Diese Verpflichtung gilt in gleichem Maße auch für eventuell beauftragte Unterauftragnehmer. Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismäßig hohen Aufwand verursachen würde, sowie Kopien, die zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.
Für diese Daten ist die Verarbeitung gem. Art. 18 DSGVO einzuschränken. Die Daten dürfen durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden und sind nach Ablauf der Aufbewahrungsfrist unverzüglich sicher zu löschen. Der Auftraggeber ist über Art und Umfang dieser gespeicherten Daten zu unterrichten. Der Auftragnehmer kann diese Daten zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.
Der Auftragnehmer hat in Abstimmung mit dem Auftraggeber nach Beendigung dieses Vertrages die gespeicherten personenbezogenen Daten in maschinenlesbarer Form bereitzustellen bzw. sicher zu löschen. Die sichere Vernichtung aller in seinem Besitz befindlichen Unterlagen schriftlich zu bestätigen.

15 Haftungsbeschränkung

Der Auftragnehmer haftet für Schäden, gleich aus welchem Rechtsgrund (z.B. Schäden aus Verletzung von vertraglichen oder vertraglichen Pflichten, Pflichtverletzungen, Delikt) wie folgt:

- Im Falle der Verletzung des Lebens, des Körpers oder der Gesundheit, bei Ansprüchen nach dem Produkthaftungsgesetz und in anderen Fällen, in denen die Haftung vom Auftragnehmer nach zwingendem Recht nicht ausgeschlossen oder beschränkt werden kann, haftet der Auftragnehmer nach den gesetzlichen Bestimmungen.
- Im Falle von Schäden, die vorsätzlich verursacht wurden, haftet der Auftragnehmer nach den gesetzlichen Bestimmungen.
- Bei grober Fahrlässigkeit der gesetzlichen Vertreter und leitenden Angestellten vom Auftragnehmer haftet der Auftragnehmer nach den gesetzlichen Bestimmungen.

- Bei leichter Fahrlässigkeit, die zur Verletzung einer Kardinalspflicht führt, ist die Haftung vom Auftragnehmer auf den vertragstypischen, bei Vertragsschluss vorhersehbaren Schaden begrenzt. Auftraggeber und Auftragnehmer sind sich darüber einig, dass die vertragstypischen und vorhersehbaren Schäden in keinem Fall über die Gesamtbeträge, die tatsächlich für die Dienste der letzten zwölf (12) Monate, die unmittelbar vor dem Ereignis entstanden sind, hinausgehen.

Es besteht keine verschuldensunabhängige Haftung, das heißt verschuldensunabhängige Haftung (z.B. gemäß § 536a Abs. 1 BGB – Bürgerliches Gesetzbuch - falls zutreffend), für Schäden, die aus Fehlleistungen resultieren, die zum Zeitpunkt des Abschlusses dieses Rahmenvertrags oder Ihrer Bestellung vorliegen.

16 Schlussbestimmungen

Sollte eine Bestimmung dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, so bleiben deren übrige Bestimmungen davon unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung tritt eine andere wirksame und durchführbare Bestimmung, welche die Parteien vereinbart hätten, wenn sie bei Abschluss dieser Vereinbarung die Unwirksamkeit oder Undurchführbarkeit der jeweiligen Bestimmung bedacht hätten und welche den Absichten der Parteien im Hinblick auf Sinn und Zweck der Vereinbarung entspricht.
Änderungen und Ergänzungen dieser Vereinbarung und ihrer Anlagen bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis.
Es gilt deutsches Recht. Gerichtsstand ist Frankfurt Oder.

Bestand der Vereinbarung werden folgende Anlagen:

- Anlage 1 | Unterauftragnehmer
- Anlage 2 | Autorisierte Personen
- Anlage 3 | Datensicherheitskonzept NET-Booking
- Anlage 4 | TOM i.S.d. Art 32 DSGVO

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Stempel/Unterschrift	Stempel/Unterschrift Geschäftsführer
…….. (Auftraggeber)	 (Auftragnehmer)

Anlage 1

Unterauftragnehmer

Die nachfolgende Liste zeigt die Unterauftragnehmer auf, welche im Rahmen der Dienstleistungen gemäß Nr. 1 der Vereinbarung Datenschutz für den Auftragnehmer tätig werden.

Unterauftragnehmer	Anschrift	Dienstleistung/Tätigkeit
Vautron Rechenzentrum AG	Obermünsterstr. 9 D- 93047 Regensburg	Hosting und Betrieb des Rechenzentrums in Regensburg / Deutschland
PC-Tutor IT-Systemhaus GmbH	August-Borsig-Ring 1 D-15566 Schöneiche	Kundenverwaltung, CRM Software

Anlage 2

Autorisierte Personen

Folgende Mitarbeiter des Auftraggebers sind weisungsberechtigt:

…… Tel.: ……

…… Tel.: ……

…… Tel.: ……

Datenschutzbeauftragter des Auftraggebers (inkl. Kontaktdaten):

……

Folgende Mitarbeiter des Auftragnehmers sind Weisungsempfänger:

Hartmut Brause	hbrause@t-online.de	Tel: 030 / 64 38 98 38
Uta Brause	ub@astrotel.net	Tel: 030 / 64 38 98 38
Torsten Brause	tb@astrotel.net	Tel: 030 / 64 38 98 38
Grit Brause	gb@astrotel.net	Tel: 030 / 64 38 98 38
Sabrina Findeisen	sf@astrotel.net	Tel: 030 / 64 38 98 38
Mandy Klapproth	mk@astrotel.net	Tel: 030 / 64 38 98 38
Charleen Bittroff	chb@astrotel.net	Tel: 030 / 64 38 98 38

Datenschutzbeauftragter des Auftragnehmers (inkl. Kontaktdaten):

DSBextern.de, Stefan Spörrer Hofbauerstraße 3a, D-94209 Regen Tel: 09921-807780 E-Mail: stefan.spoerrer@dsbextern.de

Datensicherheitskonzept

Für das Buchungssystem NET.Booking / Zimmerpfadfinder24

1 Geschäfts- und System-Context

Über das Online-Buchungssystem für Unterkünfte können verschiedene Leistungen und Produkte (Objekte) verwaltet und online gebucht werden.
Die Objekte werden vom Auftraggeber eingestellt, beschrieben und verwaltet.
Voraussetzung zur Benutzung des Systems ist ein PC, Laptop oder mobiler Computer mit einer Browseranwendung nach aktuellem technischen Standard, sowie ein Internetzugang.
Die Objektdaten, Beschreibungen und Preise werden im Internet über eine Online-Buchungsmaske, Widget oder IFrame auf der Webseite des Auftraggebers veröffentlicht.
Besucher der Webseiten haben die Möglichkeit die Daten abzurufen eine unverbindliche Online-Anfrage oder verbindliche Online-Buchung durch Eingabe Ihrer persönlichen Daten abzuschließen.
Das Buchungssystem ist eine mandantenfähige Software-as-a-Service (SaaS) Anwendung, deren Komponenten auf Servern in Partner-Rechenzentren betrieben werden. Das Buchungssystem wird als einheitlicher Service online bereitgestellt. Der Auftraggeber kann nach dem Erstellen eines Accounts die vereinbarten Funktionen nutzen, in dem er die vom Auftragnehmer benannte Internetadresse zum Verwaltungsbereich der Software aufruft und sich anmeldet.
Der Auftraggeber erhält einen Benutzerzugang, um Konfigurationen und
Inhalte des Auftraggebers und der Nutzer (Stamm- und Bewegungsdaten) eigenverantwortlich im Online-Buchungssystem einzupflegen, zu verändern und zu löschen.

2 Datenschutz

Wir legen größtmöglichen Wert auf den Schutz Ihrer Daten. Wir verpflichten uns, alle Ihre Daten, soweit dies mit technisch und wirtschaftlich vertretbarem Aufwand möglich ist, wirksam gegen unberechtigten Zugriff, Veränderung, Zerstörung, Verlust oder Missbrauch zu sichern. Bitte beachten Sie folgende Richtlinien zum Datenschutz.
Durch Ihre Nutzung des Buchungssystems NET.booking / Zimmerpfadfinder24 erhalten wir Zugang zu Ihren
persönlichen Daten. Bei der Verarbeitung personenbezogener Daten handeln wir in Ihrem Auftrag und sind verpflichtet, Ihren Weisungen zu folgen. Die Weisung bedarf der Schriftform. Die Verarbeitung oder Nutzung der überlassenen Daten wird ohne eine schriftliche Weisung weder für eigene Zwecke noch für Zwecke Dritter erfolgen
und es wird Dritten auch nicht der Zugang zu diesen Daten ermöglicht werden.
Für die Zulässigkeit der Datenerhebung und Datenverarbeitung sowie für die Wahrnehmung der Rechte der Endkunden, Nutzer und Mieter (Nutzer) ist der Auftraggeber verantwortlich.
Alle Vertragsparteien und deren Mitarbeiter sind verpflichtet, die in diesem Vertragsverhältnis erlangten Informationen während der Dauer sowie nach Beendigung vertraulich zu behandeln sowie ohne die vorherige schriftliche Zustimmung der betroffenen Partei nicht zu verwerten, zu nutzen oder Dritten zugänglich zu machen.
Beide Parteien informieren die andere Partei unverzüglich, über Offenlegung oder Verlust vertraulicher Informationen, sobald davon Kenntnis erlangt wird.

2.1 Protokolldateien

In Log-Dateien auf dem Webserver speichern wir automatisch Informationen, welche der Browser eines Nutzers an uns übermittelt. Dies sind Browsertyp/ -version, verwendetes Betriebssystem, URL der verlinkenden Seite, IP-Adresse und Uhrzeit der Serveranfrage. Diese Daten können nicht bestimmten Personen zugeordnet werden. Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen. Ohne ausdrückliche Weisung des Auftraggebers werden zur Verarbeitung der Daten des Auftraggebers weder im Frontend noch im Backend des Auftraggebers analytische Tools wie Google Analytics installiert oder eingesetzt. Die Bestellung von Leistungen eines Rechenzentrums im Namen des Auftraggebers erfolgt ebenfalls ohne den Einsatz von Google Analytics.

2.2 Rechenzentrum

Die Verarbeitung und Speicherung der überlassenen Daten erfolgt auf Webservern in der EU.
Wenn keine anderen Vereinbarungen getroffen wurden, wird das Rechenzentrum betrieben von Vautron Rechenzentrum AG.
Die Beschreibung der Datensicherheit im Rechenzentrum können bei Bedarf vom Rechenzentrum angefordert werden.
Die Installation, Einrichtung der Server und Konfiguration erfolgt durch Astrotel Internetmarketing GmbH, ihrer Mitarbeiter oder Subunternehmer.

2.3 Personal zur Administration des Buchungssystems

Wir setzen nur Mitarbeiter ein, die auf das Datengeheimnis und den Datenschutzrichtlinien verpflichtet sind. Dies gilt für interne und externe Mitarbeiter. Wir vergeben Zugriffsberechtigungen für gespeicherte Daten nur an Mitarbeiter in dem für die jeweilige Aufgabe erforderlichen Umfang. Scheidet ein Mitarbeiter aus unserem Unternehmen aus oder wird der Dienstvertrag beendet, werden die Systemzugänge und Zugriffsberechtigungen dieses Mitarbeiters unverzüglich gelöscht.
Zur Sicherung des Datenschutzes und der Einhaltung der Richtlinien der Datensicherheit für die Mitarbeiter des Auftraggebers, die das Buchungssystem benutzen und administrieren, ist der Auftraggeber selbst verantwortlich.
Wir verpflichten uns, keine Kopien oder Ausdrucke von den Daten anzufertigen, die nicht im Zuge einer ordnungsgemäßen Vertragsausführung und Betrieb der Software zwingend notwendig sind. Für die Erstellung einer Kopie zu diesem Zweck werden die persönlichen Daten des Auftraggebers und seiner Kunden wie Namen, Anschriften, E-Mail Adressen und Telefonnummern zusätzlich anonymisiert und unkenntlich gemacht.

Zugangsdaten

Der Zugang zur Administration der Vautron Serverarchitektur ist nur mit einer Zertifizierung per Benutzernamen und Passwort möglich.
Der Zugang eines Systemadministrators zum Filesystem des Webservers erfolgt ausschließlich per SSH. Der Zugang eines Systemadministrators zur Datenbank erfolgt ebenfalls ausschließlich getunnelt über den SSH Zugang.

2.4 Subunternehmen

Wir setzen externe Subunternehmer ein, die uns bei der Bereitstellung des Buchungssystems und seinen Funktionen unterstützen oder deren Software wir verwenden. Subunternehmer erhalten keinen Zugriff auf Kundendaten, wenn dies nicht für die Ausführung ihrer vertraglichen Leistung erforderlich ist. Darüber hinaus setzen wir nur solche Subunternehmer ein, denen wir vertrauen und deren Einsatz wir mit angemessenen vertraglichen
Schutzmaßnahmen absichern, wie im Abschnitt " Personal zur Administration des Buchungssystems" beschrieben.
Das Buchungssystem ist auch mit anderen Services verbunden, die direkt durch Dritte erbracht werden (z.B. Internetdienstanbieter). Diese Dritten bleiben für ihr eigenes System verantwortlich, einschließlich der Sicherheit, und der Auftragnehmer ist nicht für die Aktivitäten dieser Dritten verantwortlich.

2.5 Auskunft über gespeicherte Daten

Sie haben jederzeit das Recht auf Auskunft über die bezüglich Ihrer Person gespeicherten Daten, deren Herkunft und Empfänger sowie den Zweck der Speicherung. Auskunft über die gespeicherten Daten erteilen wir nur schriftlich an die bei uns hinterlegte Anschrift des Auftraggebers oder eines anfragenden Nutzers. Anfragen können per E-Mail an datenschutz@astrotel.net gerichtet werden. Sind Sie aufgrund geltender datenschutzrechtlicher Bestimmungen gegenüber einer Person verpflichtet, Auskünfte zur Verarbeitung oder Nutzung von Daten dieser Person zu geben, unterstützen wir Sie dabei.

3 Anwendungssicherheit

Der Auftragnehmer stellt in den Buchungssystemen verschiedene Werkzeuge zur Konfiguration der Anwendung und Anwendungssicherheit bereit. Der Auftraggeber ist für die Einrichtung und die Konfiguration der Inhalte der Benutzersicherheit verantwortlich.

3.1 Benutzerrollen

Im Standardfunktionsumfang gibt es für den Auftraggeber einen Adminbenutzer. Dem sind die Berechtigungen zur Konfiguration zugewiesen. Zusätzlich haben die Supportmitarbeiter vom Auftragnehmer persönliche Accounts mit Administrationsrechten, um den Auftraggeber bei der Problemlösung zu unterstützen.

3.2 Authentifizierung der Benutzer

Der Login in den Administrationsbereich erfolgt über die URL z.B. https://hotel-net-booking.secure4all.de/passwort.php
https://fewo-net-booking.secure4all.de/passwort.php

4. Technische Sicherheit

4.1 Verschlüsselung der Übertragung

Zur Verschlüsselung der Übertragung wird SSL Verschlüsselung RSA eingesetzt. Verschlüsselt wird dabei ab dem Zugang zum Backend über die URL https://hotel-net-booking.secure4all.de/passwort.php

https://fewo-net-booking.secure4all.de/passwort.php
Bei der Arbeit im Verwaltungsbereich werden die Daten zum Internetbrowser der Mitarbeiter des Auftraggebers verschlüsselt.
Für die Integration des Buchungsfrontends in die eigene Website des Auftraggebers wird ebenfalls eine URL basierend bereitgestellt, z.B. https://hotel-net-booking.secure4all.de/buchung/?id_hvz=3455&comeFrom=mk&form=inquiry
Zur nahtlosen Verschlüsselung der Daten vom Browser des Nutzers über die Webseite des Auftraggebers hin zum Buchungsfrontend des Buchungssystems, muss die Webseite des Auftraggebers, in welcher das Buchungsfrontend eingebunden wird, ebenfalls durch SSL verschlüsselt sein.
Ist dies der Fall, kann die Verschlüsselung zum Buchungssystem aktiviert werden, in dem die Frontend URL beginnend mit **https://** eingebunden wird.
Die Daten der Nutzer werden damit über eine verschlüsselte Verbindung vom Buchungsfrontend zum Server übertragen.

4.2 Speicherung personenbezogener Daten

In dem Buchungssystem NET.Booking / Zimmerpfadfinder24 werden Name, Anschrift und die Kontaktdaten vom Auftraggeber gespeichert. Personenbezogene Daten von Kunden des Auftraggebers werden im Rahmen einer Buchung oder Buchungsanfrage erfasst und an den Auftraggeber weitergeleitet. Diese Daten werden nicht im Buchungssystem gespeichert.

4.3 Datensicherungen

Backups des Dateisystems und der Datenbank werden täglich durchgeführt.
Die Backups werden über die Backup-Funktion des Servers durchgeführt und verbleiben innerhalb der Serverinfrastruktur und werden dort gespeichert.

Datensicherheitskonzept

für das Buchungssystem NET.Booking / Zimmerpfadfinder24
Stand Juni 2018

Astrotel Internetmarketing GmbH
Leipziger Straße 1
D-15566 Schöneiche
E-Mail: datenschutz@astrotel.net
Telefon: +49 / (0) 30 / 64 38 98 38
Fax: +49 / (0) 30 / 64 38 98 39
Geschäftsführer Dipl. Ing. Hartmut Brause

Anlage 4
Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO
Betreffend Hostingleistungen der Astrotel Internetmarketing GmbH
(d.h. Zugriffe im Rahmen der Projektierung, Fehleranalyse, Entwicklung, Pflege und Remotesupport)
Stand 07.06.2018

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn Ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1 Zutrittskontrolle

Der allgemeine Zutritt zum Gebäude erfolgt über eine Sicherheitsschließanlage.

1.2 Zugangskontrolle

Für die Anmeldung an die Mitarbeiter-PCs und Server ist ein Kennwort erforderlich.
Grundsätzlich und soweit nicht technisch notwendig, ist ein Zugang zu Auftragsdaten nur mittels personifizierten Accounts zugelassen.
Das System wird durch eine Firewall ständig überwacht. Es gibt eine Antivirus-Software auf Systemebene. Darüber hinaus ist für das Mail-System eine Antivirus-Software je Client sowie Server installiert. Es werden ausschließlich IT-Systeme eingesetzt, die vom Hersteller durch regelmäßige Sicherheitsupdates unterstützt werden.

1.3 Zugriffskontrolle

Die Zugriffskontrolle ist in differenzierten Berechtigungen auf Menü-Ebene eingerichtet.

2. Integrität (Art. 32 Abs. 1.lit. b DSGVO)

2.1 Weitergabekontrolle

Der Transport außerhalb des Unternehmensstandorts des Auftragnehmers erfolgt auf passwortgeschützten Geräten. Außerdem erfolgt eine Bereitstellung der Daten in einem Google Drive Laufwerk.

2.2 Eingabekontrolle

Alle Serveran- und abmeldungen sowie sämtliche Transaktionen auf Dateiebene (z.B. Neuanlagen, Veränderungen, Löschungen) werden protokolliert. Die Protokolle werden hinsichtlich unberechtigter Zugriffe analysiert und nach 6 Monaten gelöscht.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1.lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Es wird ein wöchentliches Backup (Vollsicherung) durchgeführt. Dazu wird zusätzlich täglich inkrementell gesichert. Die Sicherung erfolgt in zwei räumlich getrennten Bereichen auf entsprechenden Storage Systemen.
Es wird ein RAID-verfahren bei den Festplattensicherungen eingesetzt. Unterbrechungsfreie Stromversorgung (USV) samt Überspannungsschutz ist vorhanden.
Durch den Einsatz der Firewall und der Antivirus-Software für das Mail-System und alle Server, sowie Antivirus-Software je Client wird die Verfügbarkeit technisch bestmöglich sichergestellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO,Art. 25 Abs. 1 DSGVO)

4.1 Datenschutzmanagement

Alle Mitarbeiter des Auftragnehmers sind auf das Datengeheimnis verpflichtet. Es erfolgt eine regelmäßige Unterweisung der Mitarbeiter im Datenschutz. Ein Datenschutzkonzept wurde erstellt.
Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach. Für die Bearbeitung von Auskunftsanfragen seitens Betroffener existiert ein formalisierter Prozess. Für die eingesetzten IT-Systeme und Prozesse existieren Verarbeitungsverzeichnisse. Die Wirksamkeit unserer technischen Schutzmaßnahmen wird regelmäßig überprüft.

4.2 Incident-Response-Management

Firewalls, Spamfilter und Virenscanner werden eingesetzt und regelmäßig aktualisiert. Daneben existieren Systeme zur Intrusion Detection und Prevention. Eine Policy regelt den Umgang mit Sicherheitsvorfällen. Es gibt Alarmpläne und eine Dokumentation von Sicherheitsvorfällen und Datenpannen. In Abstimmung mit dem Geschäftsführer erfolgt die Meldung gegenüber den Aufsichtsbehörden.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die Prozesse für Softwarepflegeleistungen, die im Zusammenhang mit personenbezogenen Daten stehen, sind klar definiert und die involvierten Mitarbeiter sind per bindender Arbeitsanweisung entsprechend verpflichtet. Die Mitarbeiter sind angehalten nicht mehr personenbezogene Daten zu erheben, als für den jeweiligen Zweck erforderlich sind.

4.4 Auftragskontrolle (Outsourcing an Dritte)

Unsere Mitarbeiter kennen den Datenverarbeitungszweck. Sie erhalten Weisungen zum Umgang mit personenbezogenen Daten. Spezielle Unterauftragsverhältnisse (Subunternehmer) werden schriftlich beauftragt und sind im Anhang aufgeführt.