Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO

Zwischen Billbee GmbH

Arolser Straße 10

34477 Twistetal

Deutschland

E-Mail: support@billbee.de

- nachfolgend "Auftragnehmer / Auftragsverarbeiter" genannt -

und Auftraggeber

LPM e.K, Vitali Liberov, Hugo-Distler-Str. 62, 90411 Nürnberg

- nachfolgend "Auftraggeber / Verantwortlicher" genannt -

wird folgender Vertrag geschlossen:

I Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung und deren Durchführung ein Auftragsverarbeitungsvertrag (nachstehend "Vertrag" genannt) im Sinne des Art. 28 EU-Datenschutz-Grundverordnung (nachstehend "DSGVO"genannt) eingegangen. Um in Ergänzung zu der Leistungsvereinbarung die hieraus resultierenden datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien hinsichtlich der Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter im Auftrag des Auftraggebers gemäß den gesetzlichen Verpflichtungen zu konkretisieren, schließen die Vertragsparteien den nachfolgenden Vertrag.

II Anwendungsbereich

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter allein verantwortlich ("Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO). Dieser Vertrag findet Anwendung auf alle Tätigkeiten des Auftragsverarbeiters bei denen durch den Auftragsverarbeiter oder durch ihn beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

III Gegenstand und Dauer der Auftragsverarbeitung

1. **Gegenstand und Spezifizierung der Auftragsverarbeitung**

   Der Auftragsverarbeiter verarbeitet im Rahmen dieses Auftrages personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages. Aus dem Leistungsvereinbarung ergeben sich Gegenstand und Dauer der Auftragsverarbeitung. Eine Spezifizierung, sowie Art und Zweck der Auftragsverarbeitung, werden im **Anhang "Gegenstand der Auftragsverarbeitung "** konkretisiert.

2. **Räumlicher Anwendungsbereich**

   Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

3. **Dauer der Auftragsverarbeitung**

   Der Vertrag beginnt mit Unterzeichnung beider Vertragsparteien. Die Laufzeit richtet sich nach der Laufzeit des zugrundeliegenden Vertragsverhältnisses zwischen dem Auftraggeber und Auftragnehmer, sofern sich aus den Bestimmungen dieses Vertrags nicht darüber hinausgehende Verpflichtungen ergeben.

IV Pflichten des Auftragsverarbeiters

1. **Einhaltung des geltenden Rechts**

   Die Pflichten des Auftragsverarbeiters bei der Datenverarbeitung ergeben sich aus diesem Vertrag und dem anwendbaren Recht. Das anwendbare Recht umfasst insbesondere das Bundesdatenschutzgesetz („**BDSG**“) und die Datenschutz-Grundverordnung („**DSGVO**").

2. **Verarbeitung nur nach Weisung**

   Soweit dieser Vertrag Anwendung findet, wird der Auftragsverarbeiter die personenbezogenen Daten des Auftraggebers nur auf dokumentierte Weisung des Auftraggebers verarbeiten, die durch die Leistungsbeschreibung definiert sind. Der Auftraggeber kann zusätzliche Weisungen aussprechen, soweit dies zu Einhaltung des anwendbaren Datenschutzrechts erforderlich ist.

3. **Verpflichtung zur Vertraulichkeit**

   Der Auftragsverarbeiter gewährleistet, 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.

4. **Unterstützung bei der Wahrung der Betroffenenrechte**

   Der Auftragsverarbeiter wird dem Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei dessen Pflichten unterstützen, Ansprüche auf Korrektur, Löschung oder Sperrung nach dem BDSG zu beantworten bzw. Anträge auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Personen zu bearbeiten. Wenn sich ein Betroffener hinsichtlich solcher Daten, die der Auftragsverarbeiter im Auftrag des Auftraggebers verarbeitet, zwecks Geltendmachung von Betroffenenrechten unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

5. **Unterstützung bei der Einhaltung von Art. 32 - 36 DSGVO**

   Der Auftragsverarbeiter wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten im Rahmen der eigenen Möglichkeiten unterstützen, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Datenschutz-Folgeabschätzung und der Konsultation mit Aufsichtsbehörden.

6. **Bestellung eines Datenschutzbeauftragten**

   Der Auftragsverarbeiter hat folgenden betrieblichen externen Datenschutzbeauftragten bestellt: Marc Oliver Giel, Lagerstraße 11a, 64807 Dieburg. E-Mail: privacy @ billbee.io

V Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist im Rahmen dieses Vertrags allein für die Einhaltung aller Datenschutzgesetze (insbesondere der DSGVO und des BDSG) sowie dafür, dass die Datenverarbeitung und die Datenweitergabe an den Auftragsverarbeiter rechtmäßig ist und die gesetzlichen Rechte der betroffenen Personen hinsichtlich ihrer personenbezogenen Daten gewahrt wird ("Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO).
2. Insbesondere ist der Auftraggeber verantwortlich dafür, dass die vom Auftragsverarbeiter für diese Verarbeitung erstellten und jeweils aktuell geltenden, vertraglich vereinbarten technisch und organisatorischen Maßnahmen (nachstehend "**TOM**" genannt") für die Risiken der verarbeitenden Daten ein angemessenes Schutzniveau bieten.
3. Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
4. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragsverarbeiter darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Geschäftspartner und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.

5. Der Auftraggeber behält im Verhältnis zum Auftragsverarbeiter sämtliche Rechte an den auf Grundlage dieses Vertrags verarbeiteten personenbezogenen und sonstigen Daten, an überlassenen Datenträgern und überlassenen sowie zur Erfüllung dieses Vertrags geschaffenen Unterlagen.

VI Weisungen

1. Der Auftragsverarbeiter - und jede ihr unterstellte Person - darf die personenbezogenen Daten nur im Rahmen von Weisungen des Auftraggebers verarbeiten, es sei denn, es liegt eine Ausnahme nach Art. 28 Abs. 3 Satz 2 lit. a DSGVO oder nach einer anderen vorrangigen Rechtsnorm vor.
2. Die Weisungen werden anfänglich durch die Leistungsvereinbarung sowie diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form an den Auftragsverarbeiter erteilt werden ("Einzelweisung"). Mündliche Weisungen sind nur in Eilfällen gestattet und durch den Auftraggeber unverzüglich schriftlich zu bestätigen.
3. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen einschlägige Gesetze verstößt. Der Auftragsverarbeiter ist berechtigt, die Umsetzung der Weisung solange auszusetzen, bis sie vom Auftraggeber nach Überprüfung bestätigt oder abgeändert wurde.
4. Ist eine Einzelweisung nach Absatz 2 nicht vom vertraglich vereinbarten Leistungsumfang gedeckt, wird sie als Antrag auf Leistungsänderung behandelt. In diesem Fall teilt der Auftragsverarbeiter dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, Termine und Vergütung ergeben. Für den Fall, dass dem Auftragsverarbeiter die Umsetzung der Einzelweisung unter Berücksichtigung seiner berechtigten Interessen nicht zumutbar ist, ist er zur Ablehnung der Weisung berechtigt. Besteht der Auftraggeber dennoch auf die Umsetzung der Einzelweisung, steht ihm ein Sonderkündigungsrecht mit sofortiger Wirkung zu.
5. Der Auftraggeber nennt dem Auftragsverarbeiter den oder die Ansprechpartner für die Erteilung von Weisungen ausschließlich berechtigten Personen unverzüglich nach Vertragsabschluss. Für den Fall, dass keine weisungsberechtigte Person benannt wird, sind ausschließlich vertretungsberechtigte natürliche Personen des Auftraggebers zur Erteilung von Weisungen berechtigt. Der Auftragsverarbeiter ist berechtigt, die Ausführung von Weisungen bis zum Nachweis der Vertretungsberechtigung auszusetzen.
6. Weisungen in Textform sind an folgende E-Mail-Adresse zu senden: support@billbee.io

VII Technisch-organisatorische Maßnahmen

1. Der Auftragsverarbeiter wird in seinem Verantwortungsbereich den Arbeitsalltag 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 der Datenschutzgrundverordnung (Art. 32 DSGVO) genügen.
2. Der Auftragsverarbeiter 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. 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.
3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
4. Bei Akzeptanz dieses Vertrags durch den Auftraggeber werden die im **Anhang "Technisch-organisatorische Maßnahmen"** dokumentierten Maßnahmen des Auftragsverarbeiters Grundlage des Vertrags.

VIII Kontrollrechte

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Kontrollen finden, soweit nicht aus dringenden Gründen angezeigt, nicht häufiger als alle 12 Monate statt.

2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine angemessene Vergütung verlangen.

IX Subunternehmer

1. Der Auftraggeber erteilt dem Auftragsverarbeiter hiermit die allgemeine Genehmigung zur Beauftragung von Subunternehmern. Die Liste der zum Zeitpunkt des Vertragsschlusses eingesetzten Subunternehmer ist im **Anhang "Subunternehmer"** einsehbar. Der Auftraggeber behandelt die Liste der Subunternehmer als vertrauliches Geschäftsgeheimnis und darf sie nicht an unberechtigte Dritte weitergeben.
2. Der Auftragsverarbeiter hat den Subunternehmern sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser zwischen den Vertragsparteien getroffene Vertrag und die gesetzlichen Vorgaben nach der DSGVO eingehalten werden können.
3. Sofern der Auftragsverarbeiter zur Erbringung der vertraglich vereinbarten Leistung weitere oder andere Subunternehmer beauftragten will, sind diese mit der gesetzlich gebotenen Sorgfalt auszuwählen und dem Auftraggeber vor Beginn der Verarbeitung in Textform mitzuteilen. Der Auftraggeber hat das Recht, aus wichtigen datenschutzrechtlichen Gründen der Einschaltung des Subunternehmers in Textform Einspruch zu erheben. Im Falle des Einspruchs ist der Auftragsverarbeiter nach eigener Wahl berechtigt, die Leistung ohne die beabsichtigte Änderung des Subunternehmers fortzusetzen oder die Leistung gegenüber dem Auftraggeber innerhalb von vier (4) Wochen nach Zugang des Einspruchs außerordentlich mit sofortiger Wirkung zu kündigen, sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragsverarbeiter unzumutbar ist.
4. Der Auftragsverarbeiter hat die Verträge mit Subunternehmen so zu gestalten, dass sie den Vorgaben des geltenden Datenschutzrechts und dieses Vertrags entsprechen. Die Subunternehmer sind vom Auftragsverarbeiter insbesondere zu verpflichten, keine weiteren oder anderen Subunternehmer ohne Einhaltung des Vertrags zu betrauen. Der Auftragsverarbeiter kontrolliert, ob hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass das anwendbare Datenschutzrecht und dieser Vertrag eingehalten werden.
5. Nicht als Subunternehmerverhältnisse im Sinne der vorstehenden Regelungen sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z. B. Telekommunikationsleistungen, Reinigungsleistungen, Prüfleistungen oder unter Umständen auch Wartungsleistungen. Der Auftragsverarbeiter

ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers sowie zur Sicherstellung der Vertraulichkeit auch bei fremd vergebenen Nebenleistungen gesetzeskonforme und angemessene vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

X Löschung und Rückgabe nach Beendigung der Verarbeitung

1. Mit Beendigung der Auftragsverarbeitung steht dem Auftraggeber das Recht auf Herausgabe der übertragenen personenbezogenen Daten in einem maschinenlesbaren Format oder auf Löschung gemäß der nachfolgenden Bestimmungen zu.
2. Das Herausgabeverlangen ist gegenüber dem Auftragsverarbeiter innerhalb von 30 Tagen nach Vertragsbeendigung geltend zu machen.
3. Der Auftragsverarbeiter ist berechtigt, die übertragenen personenbezogenen Daten nach Ablauf von 30 Tagen nach Vertragsbeendigung zu löschen.
4. Verlangt der Auftraggeber die Datenherausgabe, ist der Auftragsverarbeiter berechtigt, die Daten anschließend unverzüglich zu löschen.
5. Von den vorstehenden Bestimmungen ausgenommen sind Daten, hinsichtlich derer der Auftragsverarbeiter gesetzlich zur Aufbewahrung verpflichtet ist.

XI Haftung

Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis als Gesamtschuldner gegenüber der jeweiligen betroffenen Person.

Wenn der Auftragsverarbeiter und der Auftraggeber an einer Datenverarbeitung gemäß dieser Vereinbarung beteiligt sind, die bei der betroffenen Person Schaden verursacht hat, übernimmt der Auftraggeber zunächst die volle Entschädigung (oder einen anderen Ausgleich), die der betroffenen Person zusteht. Erst beim zweiten Mal, fordert der Auftraggeber vom Auftragsverarbeiter den Teil der Entschädigung der betroffenen Person, der der Verantwortung des Auftragsverarbeiters für den Schaden entspricht.

Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der er

a. seinem ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder
b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat

Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist.

XII Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiter – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, 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.
2. Für diesen Vertrag gilt das Recht der Bundesrepublik Deutschland. Der ausschließliche Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragsverarbeiters, sofern der Auftraggeber Kaufmann, juristische Person oder öffentlich-rechtliches Sondervermögen ist. Dasselbe gilt, wenn

der Kunde keinen allgemeinen Gerichtsstand in der Bundesrepublik Deutschland oder der EU hat oder der gewöhnliche Aufenthalt im Zeitpunkt der Klageerhebung nicht bekannt ist. Die Befugnis, auch das Gericht an einem anderen gesetzlichen Gerichtsstand anzurufen bleibt hiervon unberührt.

3. Dieser Vertrag ersetzt alle vorherigen oder gleichzeitigen Zusicherungen, Ansprachen, Vereinbarungen, Verträge oder Mitteilungen zwischen den Parteien, gleich ob schriftlich oder mündlich geschlossen. Die jeweils geschlossene Leistungsvereinbarung bleibt davon unberührt.

Anhang: Gegenstand der Auftragsverarbeitung,
Anhang: Technisch-Organisatorische Maßnahmen

Anhang: Gegenstand der Auftragsverarbeitung

Art der Daten

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Artikeldaten
- Bestelldaten
- Käuferdaten

Art und Zweck der Datenverarbeitung

Billbee bietet eine Auftragsabwicklung, Warenwirtschaft und Automatisierungslösung für Verkäufer, die Produkte über einen oder mehrere (Online)-Kanäle verkaufen. Billbee stellt zu diesem Zweck zum einen Schnittstellen zu Quellsystemen (Shops, Marktplätze, etc.), eigene direkt in Billbee implementierte Funktionen und Schnittstellen zu Drittsystemen (Buchhaltung, Versanddienstleister, etc.) bereit.

Kategorie der betroffenen Personen

Auftraggeber und deren Beschäftigte
Kunden und deren Beschäftigte
Lieferanten und deren Beschäftigt

1 Anhang Technisch-Organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

1.1 Gewährleistung der Vertraulichkeit

1.1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.
- Die Büroräume sind mit einer Schließanlage gesichert.
- Alle Anlagen auf denen Kundendaten gespeichert werden befinden sich bei Subunternehmern (siehe Anlage) sowie in den eigenen Büroräumen.

1.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Maßnahmen:

- Keine unbefugte Systembenutzung.
- Alle eigenen IT Anlagen sind mit sicheren Kennwörter gesichert.
- Beim Verlassen des Arbeitsplatzes wird der Desktop gesperrt.
- Kunden richten sich einen eigenen durch Passwort gesicherten Zugang zu ihrem Account ein.
- Das System erzwingt eine Mindestlänge von 8 Zeichen, wobei Zahlen UND Buchstaben enthalten sein müssen.

1.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

- Die Daten sind softwareseitig gegen unbefugtes Lesen, Kopieren, Verändern oder Entfernen gesichert.
- Benutzer können Berechtigungen für Mitarbeiterebene festlegen.
- Logins werden protokolliert.
- Zu Zwecken der Fehlerbehebung können Billbee Mitarbeiter auf Kundenaufforderung Einsicht in die vom Kunden verarbeiteten Daten nehmen.
- Zugriffe von Billbee Mitarbeitern auf Kundendaten werden vom System protokolliert.

1.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Maßnahmen:

- Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.
- Das System ist mandantenfähig und stellt softwareseitig eine Trennung der Daten der einzelnen Kunden sicher.
- Jeder Kunde kann durch sein Login identifiziert nur auf die von ihm verwalteten Daten zugreifen.

1.2 Gewährleistung der Integrität

1.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten

durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

- Der Zugriff auf alle Systeme bei Subunternehmen ist per VPN gesichert.
- Alle Datenübertragungen zwischen Billbee und externen Systemen finden ausschließlich über verschlüsselte Verbindungen statt.

1.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Die Datenverarbeitung erfolgt direkt durch den Kunden.
- Sofern mehrere Mitarbeiterzugänge angelegt sind, protokolliert Billbee, durch welchen Mitarbeiter eine Dateneingabe oder Veränderung vorgenommen wurde.

1.3 Pseudonymisierung und Verschlüsselung

1.3.1 Pseudonymisierung

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Personenbezogene Daten werden zur längerfristigen Speicherung pseudonymisiert in ein dafür vorgesehenes System übertragen.

1.3.2 Verschlüsselung

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Daten werden bei der elektronischen Übertragung oder während ihres Transports verschlüsselt übertragen. Verschlüsselungsverfahren erfolgt nach aktuellem Stand der Technik.
- Daten werden nur verschlüsselt gespeichert. Verschlüsselungsverfahren erfolgt nach aktuellem Stand der Technik.

1.4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

1.4.1 Verfügbarkeit (der Daten)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- Billbee sichert alle Kundendaten im Fünfminuten Takt auf mindestens zwei externen Systemen.
- Die Systeme der eingesetzten Subunternehmen sind per USV gegen Stromausfall gesichert.
- Eine Firewall schützt den Zugriff von außen auf alle Systeme.
- Alle Systeme sind redundant ausgelegt, so dass bei einem Ausfall einer Komponente eine andere Komponente

die Aufgaben sofort übernehmen kann.

1.4.2 Belastbarkeit (der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Keine Maßnahmen

1.4.3 Wiederherstellbarkeit (der Daten / der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Vollständige Wiederherstellung des Betriebes aus einem aktuellen Backup innerhalb von ca. zwei Stunden.

1.5 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

1.5.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Abschluss der notwendigen Auftragsdatenvereinbarungen
- Abschluss der notwendigen Standard-Vertragsklauseln
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung eines Auftrags

1.5.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Datenschutz-Management
- Bestellung eines externen Datenschutzbeauftragten
- Einhaltung der Informationspflichten gemäß Art. 13 DSGVO
- Einhaltung der Informationspflichten gemäß Art. 14 DSGVO
- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Durchführung von Datenschutzfolgeabschätzungen (bei Bedarf)
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz
- Überprüfung der Wirksamkeit der TOMs (mind. jährlich durchgeführt)
- Verpflichtung der Mitarbeiter auf das Datengeheimnis

1.5.3 Incident-Response-Management

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

- Dokumentation von Sicherheitsvorfällen
- Einsatz von Firewall und deren regelmäßige Aktualisierung
- Einsatz von Spamfilter und deren regelmäßige Aktualisierung
- Einsatz von Virenscanner und deren regelmäßige Aktualisierung

1.5.4 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

- Personenbezogene Daten werden nur zweckerforderlich erhoben

Anlage - Unterauftragnehmer

Amazon Web Services, Inc.
410 Terry Avenue North
Seattle, WA 98109
USA

https://aws.amazon.com/de/

Auftragsinhalt: Speicherung der Artikelbilder und -Dateien sowie Auftragsdokumente der Händler (S3), E-Mail Empfang und Versand (SES)

cux.io UG (haftungsbeschränkt)
Lohmühlenstr. 65
12435 Berlin

https://cux.io/

Auftragsinhalt: Analyse des Nutzerverhaltens bei der Interaktion in und mit Billbee

Databox Inc.
6 Liberty Square
Boston, MA 02109
USA

https://databox.com/

Auftragsinhalt: Internes Reporting bzw. Analyse-Tool und Erstellung von internen Dashboards

Datadog, Inc.
620 8th Avenue, Floor 45
New York, NY 10018

USA

https://www.datadoghq.com/

Auftragsinhalt: Überwachung und Monitoring der Billbee Infrastruktur und Anwendung

finAPI GmbH
Adams-Lehmann-Str. 44
80797 München

https://www.finapi.io/

Auftragsinhalt: Anbindung von Bankkonten bei Verwendung des Zahlungsabgleichs

Google LLC
1600 Amphitheatre Pkwy
Mountain View, CA 94043
USA

https://www.google.com

Auftragsinhalt: Google Translate zur Übersetzung von Artikeldaten; Google Analytics zur Webanalyse; G Suite als Groupware-Lösung (E-Mail, Kalender, etc.)

Help Scout PBC
100 City Hall Plaza, 5th Floor
Boston, MA 02108
USA

https://www.helpscout.com/

Auftragsinhalt: Nutzung von Helpscout zur Lösung von Support und Kundenanfragen, sowie zur Strukturierung des eigenen Intranets.

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen

https://www.hetzner.de/

Auftragsinhalt: Housing der eigenen Server & Backup-Systeme zum Betrieb der Plattform app.billbee.io

Mixpanel
One Front Street, Floor 28
San Francisco, CA 94111
USA

https://mixpanel.com/

Auftragsinhalt: Auswertung und Aufbereitung von Nutzungsdaten der Billbee Anwender

Refiner SAS
Rue de Penthièvre 10
Paris, 75008
Frankreich

https://refiner.io/

Auftragsinhalt: Erstellung und Auswertung von Umfragen an Billbee Nutzer

Segment, Inc.
100 California Street Suite
San Francisco, CA 94111
USA

https://www.segment.com/

Auftragsinhalt: Erfassung und Aggregation von Nutzungsdaten der Billbee Anwender

Slack Technologies, Inc.
500 Howard Street
San Francisco, CA 94105
USA

https://www.slack.com/

Auftragsinhalt: Internes Kommunikationstool

Stripe, Inc.
185 Berry Street, Suite 550
San Francisco, CA 94107

https://stripe.com/

Auftragsinhalt: Abwicklung der Gebührenzahlung je nach gewählter Zahlungsart

The Rocket Science Group LLC
675 Ponce De Leon Ave NE, Suite 5000
Atlanta, GA 30308
USA

https://www.mandrill.com/

Auftragsinhalt: Nutzung der transaktionalen E-Mail API (Mandrill) zur Kundenkommunikation

Upvoty
Hurksestraat 19
Eindhoven, AH 5652
Niederlande

https://www.upvoty.com/

Auftragsinhalt: Erfassung und Verwaltung von Erweiterungswünschen

Userlist Inc.
Roswell Road 6595
Atlanta, GA 30328
USA

https://userlist.com/

Auftragsinhalt: Versenden von transaktionalen, werblichen und automatisierten E-Mails an Nutzer