

# Vereinbarung gem. Art. 28 DS-GVO

zwischen dem/der

Furnit, Manuel Döpfer, Theophanostr. 36, 50969 Köln

- Verantwortlicher - nachstehend **Auftraggeber** genannt -

und der

Billbee GmbH, Paulinenstraße 54, 32756 Detmold

- Auftragsverarbeiter - nachstehend **Auftragnehmer** genannt

## 1. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus den zugrundeliegenden Allgemeinen Geschäftsbedingungen des Auftragnehmers über die Plattform [www.billbee.io](http://www.billbee.io) (SAAS), auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des zugrundeliegenden SAAS-Vertrages.

## 2. Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

## 3. Konkretisierung des Auftragsinhalts

(1) Im Einzelnen sind insbesondere die Daten Bestandteil der Datenverarbeitung, die in Anlage 1 aufgeführt sind.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Ausgenommen davon sind Nebenleistungen.

## 4. Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 28 Abs. 3 S. 2 lit. c, Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. 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) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(4) 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. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes

personenbezogener Daten des Auftraggebers bekannt werden.

(6) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(7) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

(8) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(9) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Jan Krause, Billbee GmbH, Paulinenstraße 54, 32756 Detmold, E-Mail: support@billbee.de benannt.

(10) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

## **5. Pflichten des Auftraggebers**

(1) Weisungen an den Auftragnehmer hat der Auftraggeber in Schriftform zu erteilen.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt Nr. 4 Abs. 8 entsprechend.

(4) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

## **6. Anfragen betroffener Personen**

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

## **7. Aufsichtsbehörden**

(1) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(2) Jede Partei informiert die andere Partei über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

## **8. Technisch-organisatorische Maßnahmen**

(1) 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 auf Anforderung 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.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 3].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

## **9. Unterauftragsverhältnisse**

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.

Alle schon zum Vertragsschluss bestehenden Unterauftragsverhältnisse sind in der Anlage 2 zu diesem Vertrag angegeben. Der Auftraggeber stimmt der Beauftragung dieser genannten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

Die Hinzuziehung weiterer oder die Ersetzung der bestehenden Unterauftragnehmer sind zulässig, soweit: der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, ob die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen eingehalten werden können. Insbesondere hat der Auftragnehmer vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat und einen betrieblichen Datenschutzbeauftragten bestellt hat, sofern dies erforderlich ist.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## **10. Kontrollrechte des Auftraggebers**

(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.

## **11. Unterstützungsleistungen des Auftragnehmers**

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen im Rahmen seiner Möglichkeiten

(2) Für vorgenannte Unterstützungsleistungen kann der Auftragnehmer eine angemessene Vergütung verlangen.

## **12. Löschung und Rückgabe von personenbezogenen Daten**

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangten 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.

(3) 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.

## **13. Haftung, Schadensersatz**

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

## **14. Rechtswahl, Gerichtsstandsklausel**

(1) Es gilt deutsches Recht.

(2) Ausschließlicher Gerichtsstand ist, sofern nicht eine Norm zwingend einen anderen Gerichtsstand anordnet, das zuständige Gericht am Sitz des Auftragnehmers. Der Auftragnehmer ist jedoch berechtigt, auch das zuständige Gericht am Sitz des Auftraggebers anzurufen.

## Anlage 1 - Verfahrensangaben

### 1. Art der Daten

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

### 2. Betroffene Personengruppen

- Kunden
- Beschäftigte
- Lieferanten

### 3. 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.

## Anlage 2 - Unterauftragnehmer

**Agile CRM, Inc.,**  
22 Heritage Blvd  
Princeton NJ 08540  
USA

<https://www.agilecrm.com/>

Auftragsinhalt: Nutzung des CRM für Vertriebs- und Marketingaktivitäten

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

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

Auftragsinhalt: Speicherung der Artikelbilder der Händler

**Bablic Ltd.**  
16 Gershon Shatz,  
Tel-Aviv  
Israel

<https://www.bablic.com/>

Auftragsinhalt: Lösung zur On-the-fly Übersetzung der Billbee Oberfläche

**Centron GmbH**  
Heganger 29  
96103 Hallstadt

<https://www.centron.de/>

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

**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

**Freshworks, Inc.**  
1250 Bayhill Drive, Suite 315  
San Bruno, California 94066

USA

<https://www.freshworks.com/>

Auftragsinhalt: Nutzung der Lösung FreshDesk zur Abwicklung von Support- und Kundenanfragen

**Google LLC**

1600 Amphitheatre Pkwy  
Mountain View, California 94043  
USA

<https://www.google.com>

Auftragsinhalt: Google Translate zur Übersetzung von Artikeldaten; Google Analytics zur Webanalyse

**Inline Manual Ltd**

145-157 St John Street  
London EC1V 4PW  
England

<https://inlinemanual.com/>

Auftragsinhalt: Nutzung der Lösung zum User Onboarding bzw. In-App Support

**Microsoft Corporation (Azure)**

One Microsoft Way  
Redmond, WA 98052-6399  
USA

<https://azure.microsoft.com/de-de/>

Auftragsinhalt: Speicherung der Log-Daten

**RAIDBOXES GmbH**

Friedrich-Ebert-Straße 7  
48153 Münster

<https://raidboxes.de/>

Auftragsinhalt: Hosting der öffentlichen Marketing-Webseite [www.billbee.io](http://www.billbee.io)

**Slack Technologies, Inc.**

500 Howard Street  
San Francisco, California 94105  
USA

<https://www.slack.com/>

Auftragsinhalt: Internes Kommunikationstool

**Stripe, Inc.**

California  
185 Berry Street, Suite 550  
San Francisco, California 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, Georgia 30308  
USA

<https://www.mandrill.com/>

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

## **Anlage 3 - Technisch-organisatorische Maßnahmen**

### **1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

- o Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen: Die Büroräume Paulinenstr. 54, Detmold sind mit einer Schließanlage gesichert. Alle Anlagen auf denen Kundendaten gespeichert werden befinden sich bei Subunternehmern.
- o Zugangskontrolle: 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.
- o Zugriffskontrolle: Die Daten sind softwareseitig gegen unbefugtes Lesen, Kopieren, Verändern oder Entfernen gesichert. Benutzer können Berechtigungen für Mitarbeiter ebene 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.
- o Trennungskontrolle: 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.

### **2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

- o Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Der Zugriff auf alle Systeme bei Subunternehmen ist per VPN gesichert. Alle Datenübertragungen zwischen Billbee und externen Systemen finden ausschließlich über verschlüsselte Verbindungen statt.
- o Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Die Datenverarbeitung erfolgt direkt durch den Kunden. Sofern mehrere Mitarbeiterzugänge angelegt sind, protokolliert Billbee, durch welchen Mitarbeiter eine Dateneingabe oder Veränderung vorgenommen wurde.

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

- o Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: 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.
- o Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO): Im Falle eines Ausfalls ist Billbee in der Lage eine vollständige Wiederherstellung des Betriebes aus einem aktuellen Backup innerhalb von ca. zwei Stunden durchzuführen.

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

- o Datenschutz-Management;
- o Incident-Response-Management;
- o Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- o Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers: Alle Mitarbeiter werden auf das Datengeheimnis gemäß §5 BDSG verpflichtet. Der Auftraggeber erhält im Rahmen der Auftragsdatenverarbeitung ein Kontrollrecht. Bei der Auswahl der beauftragten Dienstleister wird die Einhaltung der DS-GVO überprüft