VERTRAG ZUR AUFTRAGSVERARBEITUNG

zwischen

BEEKEEPER («Beekeeper» und «Auftragsverarbeiter»)

und

(FIRMENNAME)

Strasse Hausnr.

Stadt, Land («Kunde»)

gemeinsam als «Vertragspartei» oder «Vertragsparteien» bezeichnet.

Dieser Vertrag zur Auftragsverarbeitung («**AVV**») ist in den Abonnementvertrag für das Frontline Success System von Beekeeper und aller anderen von den Vertragsparteien in Bezug auf die Nutzung des Frontline Success System von Beekeeper durch den Kunden bezogenen unterzeichneten Verträge (der «**Vertrag**») einbezogen und bildet einen integralen Bestandteil des Vertrags, wenn die Verarbeitung Personenbezogener Daten im Rahmen des Vertrags erforderlich ist. In Fällen, in denen der Kunde den Abonnementvertrag für das Frontline Success System von Beekeeper mit einem autorisierten Dritten (wie einem autorisierten Beekeeper-Vertriebspartner), jedoch weder mit Beekeeper noch mit einem verbundenen Unternehmen von Beekeeper, abschliesst, bezieht sich jeder Verweis auf den «Vertrag» in diesem Dokument auf den Standard-Abonnementvertrag für das Frontline Success System von Beekeeper in seiner jeweils gültigen und unter beekeeper.io/legal dargelegten Fassung.

Der Auftragsverarbeiter im Rahmen dieses AVV ist jeweils das folgende verbundene Unternehmen von Beekeeper: (i) wenn sich der Hauptsitz des Kunden in Nordamerika befindet, verweist Beekeeper auf «Beekeeper USA, Inc.»; (ii) wenn sich der Hauptsitz des Kunden in Deutschland befindet, verweist Beekeeper auf «Beekeeper GmbH»; (iii) wenn weder (i) noch (ii) zutreffen, verweist Beekeeper auf «Beekeeper AG»; oder (iv) wenn eine Beekeeper-Gesellschaft auf dem Auftragsformular angegeben ist und im Widerspruch zu (i)-(iii) steht, ist das Auftragsformular massgebend.

Der Kunde schliesst diesen AVV im eigenen Namen und im durch die Datenschutzgesetze erforderlichen Umfang im Namen der verbundenen Unternehmen des Verantwortlichen ab. Dieser AVV gilt jedoch nur sofern und soweit der Auftragsverarbeiter Personenbezogene Daten verarbeitet, für die derartige verbundene Unternehmen als «Verantwortliche» im Sinne der Datenschutzgesetze erachtet werden können. Bei der Bereitstellung der Services für den Verantwortlichen im Rahmen des Vertrags verarbeitet Beekeeper Daten des Verantwortlichen im Auftrag des Verantwortlichen, weshalb die Vertragsparteien vereinbaren, die folgenden Bestimmungen in Bezug auf alle Personenbezogenen Daten einzuhalten.

Dieser AVV gilt für die Vertragsparteien sowie für die verbundenen Unternehmen von Beekeeper, Unterauftragsverarbeiter und Mitarbeitende, die in Verbindung mit dem Vertrag Personenbezogene Daten verarbeiten.

1. Begriffsbestimmungen für den AVV

Für die Zwecke dieses AVV haben die im Folgenden definierten Begriffe die für sie dargelegte Bedeutung:

«**Abonnementgebühren**» bezeichnet die Abonnementgebühren, die vom Verantwortlichen für die Nutzerabonnemente an Beekeeper zu zahlen sind.

«**Antrag einer betroffenen Person**» bezeichnet einen Antrag eines Autorisierten Nutzers auf Wahrnehmung seiner Rechte gemäss den Datenschutzgesetzen, wie das Recht auf Zugang zu, Berichtigung, Löschung oder Einschränkung der Verarbeitung seiner Personenbezogenen Daten.

«**Anwendungen von Drittanbietern**» bezeichnet Online-Anwendungen und Offline-Softwareprodukte, die dem Verantwortlichen von Dritten direkt zur Verfügung gestellt werden und die mit den Services interagieren.

«**Aufsichtsbehörde**» bezeichnet eine unabhängige Behörde der öffentlichen Hand, die dafür verantwortlich ist, die Einhaltung der Datenschutzgesetze sicherzustellen, und deren Befugnisse durch Datenschutzgesetze geregelt sind.

«**Auftragsformular**» bezeichnet ein vom Verantwortlichen und Beekeeper in Übereinstimmung mit dem Vertrag unterzeichnetes Auftragsformular, in dem die zu erbringenden Services, die anfallenden Gebühren und andere anwendbare Anforderungen aufgeführt werden.

«**Autorisierte Nutzer**» bezeichnet die Mitarbeitenden, Vertreter und unabhängigen Auftragnehmer des Verantwortlichen und/oder seiner verbundenen Unternehmen, die vom Verantwortlichen autorisiert sind, die Services zu nutzen, wie genauer im Vertrag dargelegt, und die die zum gegebenen Zeitpunkt gültigen Endnutzerbedingungen und die Datenschutzbestimmung akzeptieren.

«**Beekeeper**» bezeichnet die folgenden verbundenen Unternehmen von Beekeeper: (i) wenn sich der Hauptsitz des Kunden in Nordamerika befindet, verweist Beekeeper auf «Beekeeper USA, Inc.»; (ii) wenn sich der Hauptsitz des Kunden in Deutschland befindet, verweist Beekeeper auf «Beekeeper GmbH»; (iii) wenn weder (i) noch (ii) zutreffen, verweist Beekeeper auf «Beekeeper AG»; oder (iv) wenn eine Beekeeper-Gesellschaft auf dem Auftragsformular angegeben ist und im Widerspruch zu (i)-(iii) steht, ist das Auftragsformular massgebend.

«**Beekeeper-Daten**» bezeichnet (i) die Informationen oder Daten, die Beekeeper vom Verantwortlichen im Rahmen der Services bereitgestellt werden, (ii) die Konfiguration der Services durch den Verantwortlichen und deren Verwendung durch die Autorisierten Nutzer (einschliesslich der Metadaten, Kommunikations- und Transaktionsprotokolle) die einer De-Identifizierung oder Pseudonymisierung unterzogen und dafür freigegeben werden und die keine Identifizierung des Verantwortlichen oder der Autorisierten Nutzer möglich machen und keine Personenbezogenen Daten enthalten dürfen, (iii) aggregierte anonymisierte Einblicke in die Nutzung der Services und (iv) alle Rückmeldungen des Verantwortlichen oder der Autorisierten Nutzer bezüglich der Services (unter der Voraussetzung, dass diese keine Daten der Verantwortlichen oder vertraulichen Informationen des Verantwortlichen enthalten).

«**Betroffene Person**» bezeichnet den Autorisierten Nutzer, der dem Verantwortlichen seine Personenbezogenen Daten anvertraut, die den Datenschutzgesetzen unterliegen, auf die sich die Personenbezogenen Daten beziehen.

«**Daten autorisierter Nutzer**» bezeichnet die Personenbezogenen Daten und andere Informationen, die Beekeeper von Autorisierten Nutzern zur Verfügung gestellt und/oder die vom Kunden zum ausschliesslichen Zweck der Kontoerstellung für einen Autorisierten Nutzer, jedoch unter Ausschluss von Kundendaten und Beekeeper-Daten, in die Services eingegeben werden.

«**Daten des Verantwortlichen**» bezeichnet alle in den Kundendaten und Daten der Autorisierten Nutzer enthaltenen Daten.

«**Datenschutzbestimmung**» bezeichnet die jeweils gültige Fassung der Datenschutzbestimmung von Beekeeper unter beekeeper.io/privacy-policy.

«**Datenschutzgesetze**» bezeichnet die anwendbaren Gesetze und Vorschriften, die die Erhebung, Verarbeitung, Speicherung und Übermittlung autorisierter Personenbezogener Daten regeln, die sich aus der Europäischen Datenschutz-Grundverordnung (DSGVO), dem Schweizer Datenschutzgesetz (DSG) oder den Datenschutzgesetzen der Vereinigten Staaten, einschliesslich des California Privacy Rights Act, ergeben.

«**Datenschutzverletzung**» bezeichnet jede bekannte unbefugte oder unrechtmässige Zerstörung, Löschung, Änderung oder Offenlegung Personenbezogener Daten, den bekannten unbefugten oder unrechtmässigen Verlust Personenbezogener Daten oder Verlust des Zugangs zu ihnen.

«**Datum des Inkrafttretens**» bezeichnet das auf einem Auftragsformular, das auf die Vereinbarung verweist, angegebene Datum des Inkrafttretens, oder, falls kein Auftragsformular erstellt wurde, das Datum, an dem der Verantwortliche mit der Nutzung der Services beginnt.

«**Dienstleistungsvereinbarung**» oder «**Vertrag**» bezeichnet die zum Datum des Inkrafttretens auf beekeeper.io/legal bereitgestellte Dienstleistungsvereinbarung von Beekeeper.

«**Endnutzerbedingungen**» bezeichnet die Dienstleistungsbedingungen für Endbenutzer für das Frontline Success System wie unter beekeeper.io/legal in der jeweils aktuellen Version definiert.

«**Feedback**» bezeichnet Kommentare, Vorschläge oder sonstige Rückmeldungen, die vom Verantwortlichen oder Autorisierten Nutzern in Bezug auf die Services oder eine ihrer Funktionen an Beekeeper übermittelt werden. Feedback kann schriftlich, mündlich oder über einen anderen Kommunikationsweg erfolgen.

«**Frontline Success System**» bezeichnet die durch Beekeeper entwickelte, lizenzierte oder anderweitig zur Nutzung autorisierte interne Kommunikationssoftwareanwendung, einschliesslich der in der Präambel dieses Vertrages beschriebenen, die Beekeeper dem Kunden und den Autorisierten Nutzern ausschliesslich zur Nutzung im Rahmen der Services zur Verfügung stellt.

«**Funktionen von Drittanbietern**» bezeichnet optionale, in die Services integrierte Dienste, die von einem oder mehreren Drittanbietern, die unter beekeeper.io/legal-library/subprocessors aufgeführt sind und gelegentlich aktualisiert werden, bereitgestellt werden und auf die Beekeeper keinen Einfluss hat (z. B. Übersetzungsdienste von Google und Microsoft Bing).

«**Gebühren**» bezeichnet die Abonnementgebühren und alle weiteren in einem Auftragsformular aufgeführten Gebühren oder Kosten.

«**Geltendes Recht**» bezeichnet in Bezug auf den Verantwortlichen alle anwendbaren Gesetze, Vorschriften, Verordnungen und administrativen Regeln und Weisungen (die in Kraft sind) innerhalb der Rechtsordnung , in denen der Verantwortliche seine Geschäftstätigkeit ausübt. In Bezug auf Beekeeper bedeutet geltendes Recht alle massgeblichen Gesetze, Vorschriften, Verordnungen und administrativen Regeln und Weisungen (die in Kraft sind) in der Schweiz, der Europäischen Union und den USA.

«**Hosting-Dienste**» bezeichnet die Bereitstellung, Verwaltung und Wartung von Servern und zugehöriger Ausrüstung, die Bereitstellung von Bandbreite in den Rechenzentren und der Betrieb des Frontline Success Systems für den Zugang und die Nutzung durch Autorisierte Nutzer gemäss diesem Vertrag.

«**Kundendaten**» bezeichnet die Daten und Informationen, (i) die Beekeeper vom Kunden in Verbindung mit diesem Vertrag zur Verfügung gestellt werden; und (ii) die vom Kunden, von Autorisierten Nutzern oder von Beekeeper im Namen des Kunden eingegeben werden, die sich aus der Nutzung der Services ergeben oder anderweitig dem Zweck dienen, die Nutzung der Services durch den Kunden zu erleichtern; jedoch mit Ausnahme von Daten Autorisierter Nutzer und von Beekeeper-Daten.

«**Neue optionale Funktionen**» bezeichnet neue Funktionen des Frontline Success Systems, die der Verantwortliche wahlweise innerhalb der Services aktivieren kann.

«**Notfallwiederherstellung**» bezeichnet die derzeitige Beekeeper-Richtlinie zur Notfallwiederherstellung, die von Beekeeper gelegentlich angepasst werden kann.

«**Nutzerabonnements**» bezeichnet die vom Kunden erworbenen Nutzerabonnemente für die Anzahl Autorisierter Nutzer, die diese Autorisierten Nutzer dazu berechtigen, in Übereinstimmung mit dem Vertrag auf die Services zuzugreifen und sie zu nutzen.

«**Personal**» bezeichnet die Mitarbeitenden, Auftragnehmer, Vertreter und Berater von Beekeeper und den verbundenen Unternehmen von Beekeeper, die an den Handlungen zur Durchführung des AVV beteiligt sind.

«**Personenbezogene Daten**» sind alle in den Daten des Verantwortlichen enthaltenen Informationen, mit denen eine natürliche Person identifiziert wird oder identifiziert werden kann, sowie alle anderen Daten, bei denen es sich um «personenbezogene Daten», «persönliche Informationen», «persönlich zuzuordnende Informationen» oder ähnliche in den Datenschutzgesetzen definierte Begriffe handelt.

«**Services**» bezeichnet (i) die Nutzung des Frontline Success Systems in Übereinstimmung mit diesem Vertrag, (ii) die Nutzung von Beekeeper-Daten, (iii) die Supportleistungen und die Hosting-Dienste, (iv) den Zugang zur Beekeeper-Hosting-Plattform und (v) alle anderen Services, die Beekeeper oder seine Mitarbeiter, Vertreter oder Subunternehmer dem Kunden oder für den Kunden erbringen, die in diesem Vertrag ausdrücklich genannt oder in einem Auftragsformular aufgeführt sind; Anwendungen und Funktionen Dritter sind hier ausgeschlossen.

«**Standardvertragsklauseln**» bezeichnet: (i) im Geltungsbereich der DSGVO die Standardvertragsklauseln im Anhang des Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates («SVK EU»), (ii) im Geltungsbereich der Datenschutz-Grundverordnung des Vereinigten Königreichs die gemäss Artikel 46 Absatz 2 Buchstabe c oder d der Datenschutz-Grundverordnung des Vereinigten Königreichs übernommenen anwendbaren Standarddatenschutzklauseln («SVK UK») und (iii) im Geltungsbereich der Datenschutzgesetzes der Schweiz die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten herausgegebenen, genehmigten oder anerkannten anwendbaren Standarddatenschutzklauseln («SVK Schweiz»).

«**Supportleistungen**» bezeichnet die Supportleistungen, die von Beekeeper in Übereinstimmung mit der Dienstleistungsvereinbarung und dem jeweiligen Auftragsformular erbracht werden, jeweils in Bezug auf die Services und einschliesslich des Frontline Success Systems.

«**Unterauftragsverarbeiter**» bezeichnet jeden Rechtsträger, der vom Auftragsverarbeiter mit der Verarbeitung Personenbezogener Daten gemäss seinen Verpflichtungen aus dem AVV beauftragt wird. Eine Liste aller Unterauftragsverarbeiter findet sich unter www.beekeeper.io/legal-library/subprocessors.

«**Verantwortlicher**» bezeichnet den Kunden und (gegebenenfalls) die verbundenen Unternehmen des Kunden, die die Zielsetzungen und Methoden der Verarbeitung Personenbezogener Daten festlegen.

«**Verarbeitung**» bezeichnet alle Handlungen oder eine Reihe von Handlungen, die mit Personenbezogenen Daten oder Daten des Verantwortlichen vorgenommen werden, unabhängig davon, ob dies automatisch geschieht oder nicht. Das schliesst Handlungen wie das Sammeln, Aufzeichnen, Organisieren, Strukturieren, Speichern, Anpassen oder Ändern, Abrufen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten oder sonstiges Zugänglichmachen, Zuordnen oder Kombinieren, Einschränken, Löschen oder Vernichten ein.

«**Verbundene Unternehmen**» bezeichnet einen Rechtsträger, der direkt oder indirekt eine Vertragspartei des AVV kontrolliert, durch eine solche kontrolliert wird oder einer gemeinsamen Kontrolle mit ihr unterliegt. Für die Zwecke des Vorhergehenden bedeutet «Kontrolle» den Besitz von (i) mehr als fünfzig Prozent (50 %) der Stimmrechte zur Wahl der Vorstandsmitglieder des Unternehmens oder (ii) mehr als fünfzig Prozent (50 %) der Eigentumsanteile am Unternehmen. «Verbundene Unternehmen» bedeutet auch eine Genossenschaft: ein Unternehmen, das sich im Besitz der Nutzer befindet und von diesen kontrolliert wird und dessen Gewinne auf der Grundlage der Nutzung gerecht verteilt werden, oder ein Unternehmen, das sich im Besitz der Personen befindet und von diesen kontrolliert wird, die seine Dienste nutzen. Für die verbundenen Unternehmen des Verantwortlichen, bei denen die Services auf unterschiedlichen Tenants (Mandanten) gehostet werden müssen, können zusätzliche Gebühren anfallen, soweit nichts anderes im Auftragsformular ausgewiesen ist.

«**Vertragspartei**» bezeichnet Beekeeper oder den Verantwortlichen einzeln. Gemeinsam werden sie als die «Vertragsparteien» bezeichnet.

«**Vertrauliche Informationen**» bezeichnet Informationen jeglicher Art und in jeglicher Form, die (i) einer Vertragspartei von der anderen Vertragspartei (oder von einer Person, von der der Empfänger weiss oder vernünftigerweise annehmen kann, dass sie gegenüber der anderen Vertragspartei eine Geheimhaltungsverpflichtung hat) im Rahmen oder aufgrund dieses Vertrages offengelegt oder beobachtet oder erlangt werden und (ii) entweder zum Zeitpunkt der Offenlegung oder innerhalb einer angemessenen Frist danach schriftlich als vertraulich oder eigentumsrechtlich geschützt bezeichnet werden (oder, wenn die Offenlegung mündlich oder durch Beobachtung erfolgt, von der Person, die die Informationen offenlegt oder die Beobachtung zulässt, mündlich als vertraulich oder eigentumsrechtlich geschützt bezeichnet wird) oder von einer Art ist, von der der Empfänger wusste oder vernünftigerweise hätte wissen müssen, dass sie vom Eigentümer der Informationen als vertraulich oder eigentumsrechtlich geschützt angesehen würde. Die Einzelheiten des Frontline Success Systems, der Services, der Beekeeper-Daten und die Ergebnisse von Leistungs- oder Sicherheitstests der Services stellen Vertrauliche Informationen von Beekeeper dar. Kundendaten sind die vertraulichen Informationen des Verantwortlichen. Der Begriff «vertrauliche Informationen» umfasst insbesondere keine Informationen, die: (i) öffentlich bekannt sind oder werden, sofern sie nicht durch ein zuständiges Gericht versiegelt wurden und nicht auf eine Handlung oder Unterlassung der empfangenden Vertragspartei zurückzuführen sind, (ii) sich vor der Offenlegung rechtmässig im Besitz der anderen Vertragspartei befanden und nicht direkt oder indirekt von der anderen Vertragspartei erworben wurden, (iii) der empfangenden Vertragspartei von einem Dritten, der nicht zur Geheimhaltung der Informationen verpflichtet ist, rechtmässig gegenüber einer Person oder Stelle offengelegt wurden, von der der Empfänger wusste oder von der er unter den gegebenen Umständen vernünftigerweise hätte annehmen müssen, dass sie existiert, oder (iv) von der empfangenden Vertragspartei unabhängig entwickelt wurde, wobei die unabhängige Entwicklung durch schriftliche Belege nachweisbar sein muss.

2. Rollen und Aufgaben

2.1. Bestimmen des Auftragsverarbeiters. Der Verantwortliche beauftragt den Auftragsverarbeiter damit, Personenbezogene Daten in Übereinstimmung mit dem Vertrag und diesem AVV zu verarbeiten.

2.2. Aufgaben des Verantwortlichen. Der Verantwortliche ist allein für die Einhaltung des Geltenden Rechts in Bezug auf die Nutzung der Services und die Verarbeitung Personenbezogener Daten gemäss den im Vertrag dargelegten ausdrücklichen Anweisungen verantwortlich, insbesondere für (i) die Rechtmässigkeit der Offenlegung Personenbezogener Daten gegenüber dem Auftragsverarbeiter und (ii) die Rechtmässigkeit der Beauftragung eines Auftragsverarbeiters mit der Verarbeitung Personenbezogener Daten und der Daten des Verantwortlichen gemäss des Geltenden Rechts.

2.3. Aufgaben des Auftragsverarbeiters. Der Auftragsverarbeiter:

2.3.1. verarbeitet Personenbezogene Daten in Übereinstimmung mit dem AVV und den Datenschutzgesetzen und

2.3.2. verarbeitet Personenbezogene Daten zu keinem anderen Zweck als (i) für die Erbringung der Services erforderlich ist, (ii) ihm von der verantwortlichen Stelle angewiesen wird oder von den Vertragsparteien vereinbart wurde oder (iii) durch die Datenschutzgesetze oder das anwendbare Recht vorgeschrieben ist, wobei der Auftragsverarbeiter im letztgenannten Fall den Verantwortlichen über eine solche zusätzliche Verarbeitung benachrichtigt, es sei denn, eine solche Benachrichtigung ist gesetzlich untersagt.

3. Umfang und Zweck der Verarbeitung

3.1. Zweck. Die Verarbeitung Personenbezogener Daten erfolgt für die Ausführung der Services und in Übereinstimmung mit dem Vertrag. Genauere Angaben zu Dauer, Art und Zweck der Verarbeitung, die Arten Personenbezogener Daten und die Kategorien der Daten von Betroffenen, die nach diesem AVV verarbeitet werden, finden sich in Anhang 1.

3.2. Umfang. Der Verantwortliche weist den Auftragsverarbeiter an, die folgenden Verarbeitungshandlungen an den Personenbezogenen Daten, die von dem Verantwortlichen oder von Autorisierten Benutzern bereitgestellt wurden, vorzunehmen:

3.2.1. alle Aufgaben ausführen, die für die Erfüllung des Vertrags, die Erbringung der Services oder die Verbesserung der vom Auftragsverarbeiter erbrachten Services erforderlich sind,

3.2.2. die Rechte und Pflichten des Auftragsverarbeiters aus dem Vertrag, einschliesslich der Dokumentation der Einhaltung des Vertrags durch den Auftragsverarbeiter, wahrnehmen,

3.2.3. Zugang zur Plattform gewähren und den damit verbundenen Support sowie die Dienstleistungen des Customer Success und Account Managements erbringen,

3.2.4. Personenbezogene Daten auf der Grundlage spezifischer Anforderungen des Verantwortlichen (z. B. insbesondere beim Erfüllen von Anfragen des Verantwortlichen zur Aktualisierung der Daten des Verantwortlichen) verarbeiten,

3.2.5. Personenbezogene Daten an Unterauftragsverarbeiter für die Erfüllung des Vertrags übermitteln,

3.2.6. Personenbezogene Daten zur Erfüllung der vertraglichen Verpflichtungen ins Ausland übermitteln,

3.2.7. Personenbezogene Daten auf Ersuchen des Verantwortlichen löschen, berichtigen, ändern, extrahieren oder ausgeben,

3.2.8. alle zum Nachweis erforderlichen Informationen für den Verantwortlichen bereitstellen, die zur Einhaltung seiner behördlichen Verpflichtungen erforderlich sind,

3.2.9. den Verantwortlichen bei den Prüfungen und Inspektionen des Verantwortlichen, die entweder vom Verantwortlichen, seinen Wirtschaftsprüfern oder anderen befugten Dritten durchgeführt werden, unterstützen,

3.2.10. Datenschutzverletzungen untersuchen,

3.2.11. Berichte verfassen oder spezifische Funktionalitäten für den Verantwortlichen entwickeln,

3.2.12. Pseudonymisierung, Anonymisierung, Randomisierung, Aggregation und andere Verarbeitungsschritte von Kundendaten und Daten Autorisierter Nutzer zur Bereitstellung, Verbesserung und Sicherheit der Services oder zur Generierung von Beekeeper-Daten durchführen,

3.2.13. ergänzende Aufgaben in Übereinstimmung mit dem Vertrag durchführen,

3.2.14. weitere Anforderungen des Verantwortlichen erfüllen,

3.2.15. Aufgaben in Verbindung mit bestimmten gesetzlichen Anforderungen erfüllen.

3.3. Einschränkungen. Dem Auftragsverarbeiter ist es untersagt, (i) Personenbezogene Daten ausserhalb des Geltungsbereichs des Vertrags zu verarbeiten, (ii) Personenbezogene Daten zu verkaufen oder (iii) Personenbezogene Daten an Dritte weiterzugeben, es sei denn, es handelt sich um den zulässigen Einsatz von Unterauftragsverarbeitern durch den Auftragsverarbeiter oder um eine rechtliche Anordnung.

4. Rechte und Pflichten des Auftragsverarbeiters

4.1. Personal. Der Auftragsverarbeiter hat sicherzustellen, dass das Personal des Auftragsverarbeiters, das mit der Verarbeitung Personenbezogener Daten befasst ist, über den vertraulichen Charakter der Personenbezogenen Daten informiert ist und Vertraulichkeitsvereinbarungen unterzeichnet hat. Der Auftragsverarbeiter hat ebenfalls sicherzustellen, dass der Zugriff des Personals auf Personenbezogene Daten auf diejenigen Personen beschränkt bleibt, die an der Wahrnehmung der Rechte und Pflichten des Auftragsverarbeiters im Rahmen des Vertrags, dieses AVV und an den damit verbundenen Tätigkeiten mitwirken, wobei der Umfang der Informationen und der Zugriff auf das für diese Mitwirkung erforderliche Mass zu beschränken ist.

4.2. Aussetzen der Verarbeitung. Sollte der Auftragsverarbeiter zu der Ansicht gelangen, dass eine Anweisung gegen Geltendes Recht verstösst, so hat er den Verantwortlichen unverzüglich darüber zu benachrichtigen, es sei denn, eine derartige Benachrichtigung ist durch Geltendes Recht oder eine zuständige Behörde untersagt. Der Auftragsverarbeiter ist berechtigt, die Ausführung derartiger Anweisungen auszusetzen, bis der Verantwortliche die Gesetzmässigkeit der Anweisungen belegt oder die Anweisungen entsprechend ändert.

4.3. Sicherheitsvorkehrungen.

4.3.1. Der Auftragsverarbeiter hat die folgenden Sicherheitsvorkehrungen getroffen: (i) interne Kontrollen zum Schutz Personenbezogener Daten, (ii) technische und organisatorische Massnahmen (wie in Ziffer 10 beschrieben) zum Schutz Personenbezogener Daten in Übereinstimmung mit den Datenschutzgesetzen und (iii) laufende Massnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste eingeführt.

4.3.2. Der Auftragsverarbeiter kann Änderungen an den Sicherheitsvorkehrungen vornehmen, solange die geänderten Sicherheitsvorkehrungen mindestens den gleichen Schutz Personenbezogener Daten bieten wie die ursprünglich vorgesehenen.

4.3.3. Der Auftragsverarbeiter hat ein Verfahren zur regelmässigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Vorkehrungen einzuführen, um die Sicherheit der Verarbeitung zu gewährleisten.

4.3.4. Wenn Personenbezogene Daten vom Personal des Auftragsverarbeiters ganz oder teilweise an Heimarbeitsplätzen verarbeitet werden, muss der Auftragsverarbeiter Leitlinien und Sicherheitsvorkehrungen einführen, die von seinem Personal einzuhalten sind.

4.4. Antrag einer betroffenen Person. Der Auftragsverarbeiter unternimmt wirtschaftlich vertretbare Anstrengungen, um den Verantwortlichen bei der Erfüllung von Anträgen und Ansprüchen betroffener Personen zu unterstützen.

4.5. Datenschutzverletzungen.

4.5.1. Sollte es zu einer Datenschutzverletzung kommen, hat der Auftragsverarbeiter sich darum zu bemühen, mögliche negative Folgen für Betroffene Personen abzuwehren.

4.5.2. Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich über Datenschutzverletzungen benachrichtigen. Wenn möglich, hat die Benachrichtigung spätestens 72 Stunden nach Bekanntwerden einer Datenschutzverletzung zu erfolgen.

4.5.3. Die Benachrichtigung an den Verantwortlichen über eine Datenschutzverletzung muss alle angemessenen Informationen enthalten, die dem Auftragsverarbeiter zu diesem Zeitpunkt zur Verfügung stehen, einschliesslich: (i) die Art der Datenschutzverletzung in Verbindung mit Personenbezogenen Daten und (ii) die Massnahmen, die in Reaktion auf die Datenschutzverletzung in Verbindung mit Personenbezogenen Daten ergriffen wurden oder aktuell oder im weiteren Verlauf ergriffen werden sowie (iii) die Massnahmen zur Abwehr der möglichen nachteiligen Auswirkungen auf die betroffenen Personen.

4.6. Änderung Personenbezogener Daten. Auf Anforderung durch den Verantwortlichen und sofern dies in den Geltungsbereich des Vertrags fällt, wird der Auftragsverarbeiter wirtschaftlich vertretbare Anstrengungen unternehmen, um Personenbezogene Daten zu berichtigen, zu extrahieren oder zu löschen. Der Verantwortliche trägt alle durch solche Anforderungen anfallenden Kosten.

4.7. Bei Kündigung. Bei Kündigung des Vertrags löscht der Auftragsverarbeiter die Daten des Verantwortlichen dauerhaft aus seinen Systemen und gibt dem Verantwortlichen auf Anforderung eine Kopie der Daten des Verantwortlichen zurück. Sollte der Verantwortliche besondere Anforderungen haben, die von den Standards des Auftragsverarbeiters bei der Rückgabe oder Löschung von Daten abweichen, so berücksichtigt der Auftragsverarbeiter diese nach Treu und Glauben und der Verantwortliche trägt alle durch derartige besondere Anforderungen verursachten Kosten.

4.8. Support. Der Auftragsverarbeiter wird sich in wirtschaftlich vertretbarem Umfang bemühen, dem Verantwortlichen die Informationen zur Verfügung zu stellen, die dieser benötigt, um seinen Verpflichtungen gemäss des Geltenden Rechts nachzukommen. Dies beinhaltet auch die Bereitstellung von Informationen über die Verarbeitung Personenbezogener Daten und die bestehenden Sicherheitsvorkehrungen. Der Verantwortliche trägt alle durch solche Anforderungen entstehenden Kosten gemäss dieses Paragraphen.

4.9. Aufsichtsrechtliche und gesetzliche Aufforderungen. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich über jede Aufforderung einer Behörde zur Übermittlung von Daten, die in den Geltungsbereich des Vertrags fallen, es sei denn, eine derartige Benachrichtigung ist gesetzlich oder von einer zuständigen Behörde untersagt (z.B. laut Vorschriften, die Geheimhaltung von Ermittlungen einer Strafverfolgungsbehörde gewährleisten sollen). Falls erforderlich, wird der Auftragsverarbeiter wirtschaftlich angemessene Anstrengungen unternehmen, um den Verantwortlichen bei Gesprächen mit den für die Beaufsichtigung der Datenschutzgesetze zuständigen Behörden zu unterstützen. Der Auftragsverarbeiter wird auch alle wirtschaftlich vertretbaren Vorschläge dieser Behörden zur Verbesserung der Verarbeitung Personenbezogener Daten umsetzen.

5. Rechte und Pflichten des Verantwortlichen

5.1. Unregelmässigkeiten**.** Der Verantwortliche benachrichtigt den Auftragsverarbeiter unverzüglich über alle Mängel oder Unregelmässigkeiten in Bezug auf den Datenschutz, die er in den Ergebnissen der Tätigkeiten des Auftragsverarbeiters feststellt.

5.2. Datenschutzprobleme. Der Verantwortliche benachrichtigt den in Anhang 1 dieses AVV vorgesehenen Ansprechpartner beim Auftragsverarbeiter über Probleme, die sich aus dem Vertrag oder im Zusammenhang mit ihm ergeben, wie in Anhang 1 dieses AVV aufgeführt.

6. Anträge betroffener Personen

6.1. Antragsverfahren. Wenn eine Person den Auftragsverarbeiter direkt auffordert, Auskunft über Personenbezogene Daten zu erteilen, diese zu ändern oder zu löschen (oder darzulegen, welche Kategorien Personenbezogener Daten zu welchem Zweck aufbewahrt werden), leitet der Auftragsverarbeiter diesen Antrag unverzüglich an den Verantwortlichen weiter. Hält der Verantwortliche den Antrag der Betroffenen Person für gerechtfertigt und stuft er diese Person als Betroffene Person ein, so benachrichtigt er den Auftragsverarbeiter unverzüglich und stellt eine *Beekeeper-Kundendatenanfrage* unter Angabe der genauen Anforderungen für den Auftragsverarbeiter aus. Die Kundendatenanfrage dient der Erfüllung des Antrags der betroffenen Person auf der Basis der vereinbarten Anweisungen des Verantwortlichen.

6.2. Zeitlicher Ablauf. Der Auftragsverarbeiter hat sich zu bemühen, der Kundendatenanfrage zügig und in jedem Fall innerhalb von fünfundzwanzig (25) Tagen nachzukommen. Der Auftragsverarbeiter kann die Frist in den folgenden Fällen begründet verlängern: (i) in den konkreten Fällen, die das Datenschutzgesetz vorsieht (z. B. bei einer grossen Anzahl von Anfragen oder komplexen Fällen), oder (ii) wenn das Datenschutzgesetz keine Frist oder eine Frist von mehr als dreissig (30) Tagen für die Beantwortung des Antrags der betroffenen Person durch den Verantwortlichen vorsieht. Wenn der Auftragsverarbeiter beschliesst, die Frist zu verlängern, benachrichtigt er den Verantwortlichen über diese Entscheidung unter Angabe der Gründe für die Verlängerung. Ist der Verantwortliche der Ansicht, dass die Verlängerung nach Datenschutzgesetz nicht zulässig ist, so benachrichtigt er den Auftragsverarbeiter unverzüglich darüber und die Vertragsparteien prüfen die Situation nach Treu und Glauben.

6.3. Verantwortlichkeiten. Der Auftragsverarbeiter haftet nicht dafür, dass der Verantwortliche seinen Verpflichtungen im Zusammenhang mit den Anträgen betroffener Person nachkommt, oder wenn der Verantwortliche sich weigert, diesen Anträgen nachzukommen. Der Verantwortliche trägt die alleinige Verantwortung für seine Entscheidungen über die Erfüllung solcher Anträge und stellt den Auftragsverarbeiter von allen Ansprüchen der betroffenen Person oder von Dritten frei, die aufgrund der Weigerung des Verantwortlichen, solchen Anträgen nachzukommen, entstehen.

7. Beleg von Sicherheitsvorkehrungen

Der Auftragsverarbeiter dokumentiert und belegt auf Verlangen des Verantwortlichen, dass er die in Anhang II aufgeführten Sicherheitsvorkehrungen eingeführt hat und seinen Verpflichtungen aus diesem AVV nachkommt.

8. Recht auf Prüfung und Inspektion

8.1. Jährliche Prüfungen durch den Auftragsverarbeiter. Der Auftragsverarbeiter lässt jährliche Prüfungen gemäss ISO-20017-Standards durch einen Dritten durchführen und legt dem Verantwortlichen auf Anfrage die ISO-Zertifizierung vor.

8.2. Prüfungsrecht des Verantwortlichen. Der Verantwortliche hat das Recht, bei Vorliegen eines konkreten und hinreichend abgesicherten Grundes die Einhaltung dieses AVV durch den Auftragsverarbeiter während der Vertragslaufzeit jederzeit zu überprüfen. Der Verantwortliche teilt dem Auftragsverarbeiter den vollständigen Prüfungsbericht und die Ergebnisse mit.

8.3. Umfang. Der Verantwortliche kann den Umfang der Prüfung auf bestimmte Verarbeitungstätigkeiten beschränken oder auf die gesamten Verarbeitungstätigkeiten des Auftragsverarbeiters ausdehnen. Der Verantwortliche informiert den Auftragsverarbeiter im Voraus über den geplanten Umfang der Prüfung. Der Auftragsverarbeiter kann den direkten Zugang zu Speichern und Orten, an denen die Daten anderer Kunden gespeichert werden, verweigern und von der Erteilung von Auskünften absehen, wenn durch diese die Vertraulichkeit der Daten anderer Kunden des Auftragsverarbeiters beeinträchtigt werden könnte. Der physische Zugang zu den Rechenzentren des Auftragsverarbeiters ist von jeder Prüfung oder Inspektion ausgeschlossen.

8.4. Durchführung. Der Verantwortliche kann die Prüfung selbst durchführen, oder einen externen Prüfer einsetzen. Alle an der Prüfung teilnehmenden Personen müssen eine vom Auftragsverarbeiter vorbereitete Vertraulichkeitserklärung unterzeichnen, bevor sie im Rahmen der Prüfung Inspektionen durchführen. Der Auftragsverarbeiter hat das Recht, eine Prüfung durch einen Prüfer, der ein Wettbewerber des Auftragsverarbeiters ist, abzulehnen. In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen schriftlich den Grund für die Ablehnung mit, und der Verantwortliche hat die Möglichkeit, einen anderen Prüfer auswählen.

8.5. Vorankündigung. Der Verantwortliche hat den Auftragsverarbeiter im Voraus schriftlich über den Umfang der Prüfung, den Namen des Prüfers und das vorgeschlagenen Prüfungsdatum (mindestens fünfzehn Tage nach Erhalt dieser Benachrichtigung durch den Auftragsverarbeiter) zu benachrichtigen. Der Auftragsverarbeiter unternimmt wirtschaftlich vertretbare Anstrengungen, um sein System und sein Personal zu den regulären Geschäftszeiten am vom Verantwortlichen vorgeschlagenen Prüfungsdatum oder an einem anderen einvernehmlich festgelegten Tag, der so nah wie möglich am vorgeschlagenen Datum liegt, bereitzustellen.

8.6. Kosten. Der Verantwortliche trägt die alleinigen Kosten, einschliesslich der Kosten für externe Prüfer, die zur Durchführung der vom Verantwortlichen angeforderten Prüfung anfallen. Mit Ausnahme der vom Verantwortlichen angeforderten Prüfungen nach einer Datenschutzverletzung leistet der Verantwortliche dem Auftragsverarbeiter eine Erstattung für die Zeit und die sonstigen Kosten, die diesem für die Unterstützung der Prüfung angefallen sind, wenn die Prüfung einen Zeitaufwand von mehr als fünf Stunden für die Unterstützung der Prüfung verursacht.

8.7. Häufigkeit. Sofern keine Datenschutzverletzung vorliegt, darf der Verantwortliche nur einmal pro Kalenderjahr eine Prüfung anfordern, und die Dauer der Prüfung darf drei Arbeitstage nicht überschreiten, sofern nichts anderes vereinbart wurde.

8.8. Prüfung durch eine Aufsichtsbehörde. Führt eine Datenschutzbehörde oder eine andere Aufsichtsbehörde mit gesetzlicher Zuständigkeit für den Verantwortlichen auf Antrag des Verantwortlichen eine Prüfung durch, so gelten die nachstehenden Ziffern 8.2 bis 8.6 *entsprechend*. Die Unterzeichnung einer Vertraulichkeitserklärung ist nicht erforderlich, wenn die betreffende Aufsichtsbehörde einer beruflichen oder gesetzlichen Verschwiegenheitspflicht unterliegt, deren Verletzung nach dem Geltenden Recht strafbar ist.

8.9. Alternative unabhängige Prüfung. Alternativ zur Prüfung durch den Verantwortlichen kann der Auftragsverarbeiter nach eigenem Ermessen (sofern dies nicht durch zwingende Rechtsvorschriften untersagt ist) einen unabhängigen und anerkannten externen Prüfer mit der Durchführung der Prüfung auf Kosten des Auftragsverarbeiters beauftragen. Der Auftragsverarbeiter teilt dem Verantwortlichen dann den vollständigen Prüfungsbericht und die Ergebnisse mit.

9. Unterauftragsverarbeiter

9.1. Einsatz und Änderung von Unterauftragsverarbeitern. Der Verantwortliche willigt hiermit ein und befugt den Auftragsverarbeiter, die Liste der Unterauftragsverarbeiter in Anhang 1 jederzeit zu verwenden, zu integrieren, zu erweitern, zu reduzieren, zu modifizieren oder anderweitig zu ändern. Der Auftragsverarbeiter hat den Anhang 1 entsprechend anzupassen. Jede Erweiterung des Verarbeitungsumfangs durch einen Unterauftragsverarbeiter gemäss Anhang 1 oder die Beauftragung eines neuen Unterauftragsverarbeiters (gemeinsam als «Änderungen» bezeichnet) wird für den Verantwortlichen nach einer Ankündigung der Änderungen durch den Auftragsverarbeiter mit einer Frist von mindestens sechzig (60) Tage wirksam. Die Beauftragung eines neuen Unterauftragsverarbeiters im Zusammenhang mit einer neuen optionalen Funktion erfolgt nach dem in Ziffer 9.5 beschriebenen Verfahren.

9.2. Einwände gegen Änderungen bei Unterauftragsverarbeitern.

9.2.1. Der Verantwortliche kann nach Treu und Glauben und unter Angabe von Gründen Einspruch gegen Änderungen erheben, wenn diese Änderungen die Interessen des Verantwortlichen wesentlich beeinträchtigen würden, wie z. B.: (i) bei einer Änderung der gesetzlichen Vorschriften, die den Auftragsverarbeiter dazu verpflichten würden, Personenbezogene Daten in einer Weise zu verarbeiten, die nicht mit den Anweisungen des Verantwortlichen konform ist, (ii) bei einer Änderung, die das Risiko einer Verletzung der Sicherheit Personenbezogener Daten erhöhen würde, oder (iii) bei einer Änderung, die dem Unterauftragsverarbeiter einen wesentlichen Wettbewerbsvorteil gegenüber dem Verantwortlichen verschaffen würde. Ungeachtet jeglicher gegenteiligen Bestimmungen in diesem Vertrag darf der Verantwortliche seine Zustimmung zu Änderungen bei Unterauftragsverarbeitern nicht unbegründet verweigern.

9.2.2. Der Einspruch des Verantwortlichen muss innerhalb von sechzig (60) Tagen, nachdem der Verantwortliche über die Änderung informiert wurde, beim Auftragsverarbeiter eingehen. Der Einspruch muss schriftlich erfolgen und die berechtigten Gründe des Verantwortlichen für den Einspruch darlegen sowie Gegenmassnahmen vorschlagen.

9.3. Annahme von Änderungen. Erhebt der Verantwortliche keinen Einspruch gegen die Änderung der/des Unterauftragsverarbeiter(s) gemäss Ziffer 9.2, so gilt die Änderung als vom für die Verarbeitung Verantwortlichen angenommen.

9.4. Recht des Auftragsverarbeiters auf Abhilfe. Erhebt der für die Verarbeitung Verantwortliche gemäss dem in Ziffer 9.2 beschriebenen Verfahren Einspruch gegen die Änderung, hat der Auftragsverarbeiter das Recht, Abhilfe gegen den Einspruch zu schaffen, indem er (nach alleinigem Ermessen des Auftragsverarbeiters) einen der folgenden Schritte durchführt:

9.4.1. Keine Umsetzung der Änderung,

9.4.2. Umsetzung der vom Verantwortlichen in seinem Einspruch geforderten Gegenmassnahmen oder

9.4.3. Aufforderung an den Verantwortlichen, die Nutzung der betroffenen Funktion der Services einzustellen. Der Auftragsverarbeiter hat dem Verantwortlichen die Kosten für die Entfernung einer solchen Funktion nur dann zu erstatten, wenn der Verantwortliche für diese Funktion zusätzliche, gesonderte Gebühren zahlt, die als Posten auf dem Auftragsformular aufgeführt sind. Eine derartige Erstattung wird *zeitanteilig* ab dem Zeitpunkt der Umsetzung der Änderungen berechnet.

9.4.4. Falls die vom Auftragsverarbeiter ergriffenen Massnahmen den Einspruch des Verantwortlichen gemäss Ziffer 9.2.1 nicht ausräumen und die Vertragsparteien keine gütliche Einigung nach Treu und Glauben erzielen können, ist jede Vertragspartei berechtigt, den Vertrag zu kündigen. Die Kündigung wird an dem Tag wirksam, an dem die Änderung tatsächlich umgesetzt wird.

9.5. Änderung des Unterauftragsverarbeiter für eine Neue Optionale Funktion. Die Beauftragung eines neuen Unterauftragsverarbeiters für eine Neue Optionale Funktion wird wirksam, sobald der Auftragsverarbeiter dem Verantwortlichen eine Vorankündigung über die Einführung der Neuen Optionalen Funktion hat zukommen lassen. Anhang 1 wird entsprechend aktualisiert, und die Zustimmung des Verantwortlichen für den Einsatz des neuen Unterauftragsverarbeiters ist einzuholen, wenn der Verantwortliche die Neue Optionale Funktion nutzt.

9.6. Vertragliche Verpflichtungen gegenüber Unterauftragsverarbeitern. Der Auftragsverarbeiter schliesst mit allen Unterauftragsverarbeitern Verträge ab, die alle erforderlichen vertraglichen und technischen Massnahmen zum Schutz der Personenbezogenen Daten beinhalten. Die Datenschutz- und Informationssicherheitsebene muss mindestens der Sicherheitsebene entsprechen, die der Auftragsverarbeiter im Rahmen des AVV zusagt, und darf nicht weniger Sicherheit bieten als durch die anwendbaren Gesetze vorgesehen.

9.7. An Unterauftragsverarbeiter geknüpfte Kosten. Der Auftragsverarbeiter trägt die mit dem Einsatz von Unterauftragsverarbeitern verbundenen Kosten. Verlangt der Verantwortliche jedoch vom Auftragsverarbeiter den Einsatz eines bestimmten Unterauftragsverarbeiters und ist der Auftragsverarbeiter bereit und in der Lage, eine solche Lösung anzubieten, so trägt der Verantwortliche die alleinigen Kosten (einschliesslich der internen Kosten des Auftragsverarbeiters), die an den Einsatz eines solchen Unterauftragsverarbeiters geknüpft sind.

10. Technische und organisatorische Massnahmen

10.1. Implementierung technischer und organisatorischer Massnahmen. Um den Schutz und die Sicherheit Personenbezogener Daten zu gewährleisten und die Datenschutzgesetze einzuhalten, implementiert der Auftragsverarbeiter technische und organisatorische Massnahmen, die sich unter anderem auf Speicherung, Datenverarbeitung, Netzwerk-Zugriff, Übertragung, Eingabe, Reihenfolge und Kontrolle beziehen, wie in Anhang 2 dargelegt.

10.2. Zweck der technischen und organisatorischen Massnahmen. Zweck der technischen und organisatorischen Massnahmen ist der Schutz der Personenbezogenen Daten vor versehentlicher oder unrechtmässiger Zerstörung, Veränderung, unbefugter Weitergabe oder vor Verlust, Missbrauch oder sonstiger Verarbeitung unter Verletzung des Datenschutzgesetzes.

11. Übermittlung der Daten des Verantwortlichen

11.1. Datenübermittlung ins Ausland. Der Verantwortliche ermächtigt den Auftragsverarbeiter und seine Unterauftragsverarbeiter, Personenbezogene Daten ins Ausland zu übermitteln, insbesondere aus dem EWR, der Schweiz und dem Vereinigten Königreich in die USA. Diese Übermittlungen ins Ausland erfolgen in Übereinstimmung mit den Datenschutzgesetzen, und der Auftragsverarbeiter wird bei Bedarf die gesetzlich vorgeschriebenen angemessenen Sicherheitsvorkehrungen treffen. Diese Sicherheitsvorkehrungen können unter anderem Folgendes umfassen: (i) die Übermittlung der Personenbezogenen Daten an einen Empfänger in einem Land, das laut Beurteilung durch eine Aufsichtsbehörde nach einem anerkannten Rahmen einen angemessenen Schutz für Personenbezogene Daten bietet, oder (ii) die Übertragung Personenbezogener Daten an einen Empfänger, der von der zuständigen Aufsichtsbehörde übernommene oder genehmigte Standardvertragsklauseln unterschrieben hat.

12. Rückgabe und Löschung der Daten bei Kündigung

12.1. Nach Ablauf der Vertragslaufzeit kommt der Auftragsverarbeiter keinen Anträgen von betroffenen Personen mehr nach. Der Auftragsverarbeiter führt nur die folgenden Abläufe im Zusammenhang mit den Personenbezogenen Daten des Verantwortlichen durch: dauerhafte Löschung der Personenbezogenen Daten und, falls vom Verantwortlichen ausdrücklich angefordert, Extraktion der Personenbezogenen Daten in einem maschinenlesbaren Standardformat.

12.2. Vertragslaufzeit**.** Der AVV wird mit seiner Unterzeichnung gültig und bleibt so lange in Kraft, wie der Auftragsverarbeiter Personenbezogene Daten verarbeitet, oder bis sechzig (60) Tage nach Ablauf oder Kündigung des Vertrags, je nachdem, was zuerst eintritt.

13. Sonstiges

13.1. Mitteilungen. Abgesehen von den im Vertrag vorgesehenen Bestimmungen in Bezug auf Mitteilungen gilt für Mitteilungen im Rahmen dieses AVV das folgende Verfahren:

13.1.1. Mitteilungen an den Auftragsverarbeiter. Mitteilungen an den Auftragsverarbeiter im Rahmen dieses AVV sind per anerkanntem Nachtkurier oder per Einschreiben mit Empfangsbestätigung an Beekeeper AG, Hardturmstrasse 181, 8005 Zürich, Schweiz, zu senden.

13.1.2. Mitteilungen an den Verantwortlichen. Mitteilungen an den Verantwortlichen in Bezug auf die Verarbeitung Personenbezogener Daten und zum AVV können an die E-Mail-Adresse des Datenschutzbeauftragten des Verantwortlichen oder an eine andere in Anhang 1 angegebene Kontaktperson gesendet werden. Mitteilungen des Auftragsverarbeiters an den Verantwortlichen in Bezug auf Anfragen betroffener Personen können direkt per E-Mail an die Person gesendet werden, die die Anfragen Betroffener Personen für den Verantwortlichen anfordert. Der Verantwortliche ist damit einverstanden, Mitteilungen in elektronischer Form zu erhalten. Eine solche Mitteilung gilt als schriftliche Mitteilung an den Verantwortlichen.

13.1.3. Zustellungsdatum. Mitteilungen bedürfen der Schriftform und gelten an dem Datum der Zustellungsbestätigung des Kurierdienstes, dem Datum auf der Empfangsbestätigung oder dem Datum der elektronischen Übermittlung als zugestellt. Der Verantwortliche informiert Beekeeper über die Änderung seiner Kontaktinformationen.

13.2. Elektronische Unterschrift. Die Vertragsparteien stimmen hiermit der Verwendung elektronischer Unterschriften im Zusammenhang mit der Unterzeichnung dieses AVV zu und vereinbaren ferner, dass elektronische Unterschriften zu diesem AVV rechtsverbindlich sind und dieselbe Wirkung haben wie handschriftlich ausgeführte Unterschriften.

13.3. Anwendbarkeit des Vertrags. Zur Klarstellung wird festgehalten, dass die im Vertrag festgelegten Paragraphen auch für den AVV gelten.

13.4. Widerspruch. Soweit eine der Bestimmungen dieses AVV mit den Bestimmungen des Vertrags im Widerspruch steht, sind die Bestimmungen dieses AVV massgebend.

ANHANG 1

Beschreibung von Übermittlung und Verarbeitung

a. Katalog (mit Klassifizierung nach Sensibilität) der zu übermittelnden und zu verarbeitenden Personenbezogenen Daten:

Zum Beispiel: Vorname, Nachname, E-Mail-Adresse, Telefonnummer

b. Zweck(e) der Übermittlung und Verarbeitung:

Zum Beispiel: Bereitstellung von SaaS-Services, Einarbeitung, Schulung, usw.

c. Kategorien der betroffenen Personen:

Zum Beispiel: Mitarbeitende, externe Auftragnehmer, usw.

d. Unterauftragsverarbeiter, die Zugriff auf Personenbezogene Daten haben oder solche erhalten können:

Die vollständige Liste der Unterauftragsverarbeiter von Beekeeper finden Sie auf unserer Webseite www.beekeeper.io/legal library/subprocessors

e. Weitere nützliche Informationen (hier können alle vereinbarten Definitionen festgehalten werden)

Bei Bedarf ausfüllen, ansonsten leer lassen

f. Kontaktinformationen für Datenschutzanfragen (Datenschutzbeauftragter)

BEEKEEPER Datenschutzbeauftragter	Telefonnummer/E-Mail-Adresse dpo@beekeeper.io
Datenschutzbeauftragter des Verantwortlichen oder andere Kontaktperson	Telefonnummer/E-Mail-Adresse

ANHANG 2

Vom Auftragsverarbeiter eingeführte technische und organisatorische Massnahmen

Dokumentation der technischen und organisatorischen Massnahmen, die der Auftragsverarbeiter einzuführen hat.

Beschreibung der Massnahmen zur Gewährleistung eines dem Risiko angemessenen Sicherheitsniveaus, einschliesslich *u. a*:

1. Massnahmen zur Pseudonymisierung und Verschlüsselung von Personenbezogenen Daten

Da wir bei den derzeitigen Services und Produktangeboten keine Daten ausserhalb des Produktdatenspeichers verarbeiten, setzen wir keine Pseudonymisierungsmassnahmen ein. Wir haben jedoch angemessene Kontrollen zur Verschlüsselung von Daten, einschliesslich Personenbezogener Daten, wie in unserem White Paper zur Datensicherheit definiert, eingeführt. Die Anwendung der Verschlüsselung erstreckt sich auf die Speicherung von Daten auf Mobilgeräten und in Datenbanken, die in unseren VPCs (Virtual Private Clouds) gehostet werden. Darüber hinaus werden alle Datenübertragungskanäle, soweit möglich, mit sicheren Protokollen verschlüsselt. Weitere Informationen befinden sich in unserem White Paper zur Datensicherheit.

2. Massnahmen zur Gewährleistung der durchgängigen Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Services

Wir haben eine Reihe von Massnahmen umgesetzt, um die Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Services zu gewährleisten:

- Ein Informationssicherheitsmanagementsystem (ISMS), das nach den Kontrollzielen gemäss ISO 27001/2 zertifiziert ist und durch die Standards von ISO 27017 und 27018 ergänzt wird
- Eingebettete Governance-Struktur und betriebliche Verfahren für das Risikomanagement im Bereich der operativen Informationssicherheit
- Verwendung von Zwei-Faktor-Authentifizierung und, wo möglich, Single Sign-on für alle Mitarbeitenden
- Sichere zentral verwaltete Firmenlaptops mit Verschlüsselung und Schutz durch Anti-Malware-Lösungen
- Verteilung der Rechenzentren durch VPCs (Virtual Private Clouds) auf mehrere Regionen. Alle Rechenzentrumspartner verfügen über eine ISO-27001-Zertifizierung und erfüllen weitere Anforderungen
- Schutz der VPC-Umgebung mit einer getrennten Sicherheitsarchitektur einschliesslich Firewalls an der Systemgrenze, die komplett durch Mitarbeitende von Beekeeper kontrolliert wird (White Paper Datensicherheit)
- Begrenzter Zugriff auf die Produktions-Mandanten für autorisierte Beekeeper-Mitarbeitende gemäss den Informationssicherheitsrichtlinien von Beekeeper und dem Need-to-know-Prinzip
- Formalisierter Prozess zur Kontrolle des Zugriffs auf Produktions-Mandanten durch festgelegte Kundensupport- und/oder Customer Success Manager
- Implementierung einer Lösung zur Verwaltung des privilegierten Zugriffs und anderer technischer Massnahmen zur Steuerung (Bereitstellung und Überwachung) privilegierter Infrastrukturzugriffe und des Zugriffs auf Produktionsumgebungen
- Trennung von Produktions-, Staging- und Entwicklungsumgebungen
- Bereitstellung von Admin-Bereich-Funktionen für die vollständige lokale Benutzerverwaltung durch den Verantwortlichen
- Bereitstellung einer direkten Schnittstelle zu SSO- oder AD- oder SFTP-Lösungen zur Verwaltung des Zugriffs durch berechtigte Nutzer (falls vom Verantwortlichen bereitgestellt)
- Verwendung des Push-Prinzips bei der Nutzung aller Dienste von Drittanbietern (die keinen Datenabruf initiieren dürfen)

- Festgelegtes Verfahren zur Bewertung der durch Dritte verursachten Sicherheitsrisiken
- Festgelegter und kontrollierter Change-Management-Prozess hoher Automatisierungsgrad in einer Microservices-Umgebung
- Mit sicheren Algorithmen verschlüsselte Kommunikation mit täglicher Zertifikatsüberprüfung
- Angemessene Protokollierung der Zugriffe auf die Beekeeper-Produktionsumgebung
- Strukturierte Governance zur Überprüfung und kontinuierlichen Verbesserung der Risiko- und Compliance-Kontrollen.
- Regelmäßig Fortbildung und Sensibilisierungstrainings für alle Beekeeper-Mitarbeitenden:
    I. Jährliches obligatorisches Informationssicherheitstraining und Sensibilisierungsschulung
    II. Laufender Zugang zu Sicherheitsschulungsmaterialien
    III. Jährliche obligatorische rollenbasierte Sicherheitsschulung für Ingenieure
    IV. Regelmäßige offene Sicherheitssitzungen für Entwickler (z. B. zum Thema OWASP)
    V. Vierteljährliche Schulungen zum Thema Informationssicherheit für neue Mitarbeitende
- Implementierung einer hochbelastbaren Backup- und Datenwiederherstellungslösung
- Kontinuierliche Überwachung der Serviceverfügbarkeit. Zugang zu Status-Seite für den Verantwortlichen (status.beekeeper.io)
- Vertraglich verbindliche Einhaltung der Serviceverfügbarkeit von 99,9 %
- Massnahmen zur zügigen Wiederherstellung der Verfügbarkeit und des Zugangs zu Personenbezogenen Daten im Falle eines physischen oder technischen Störfalls
- Beekeeper führt vierteljährlich szenariobasierte Disaster-Recovery-Tests durch, um die Wiederherstellbarkeitsfähigkeit verschiedener Dienste zu bewerten.

3. Prüfung, Beurteilung und Bewertung der technischen und organisatorischen Massnahmen

Prozesse zur regelmässigen Prüfung, Beurteilung und Bewertung der Wirksamkeit technischer und organisatorischer Massnahmen sind vorhanden. Beekeeper hat eine Governance-Struktur für das Risikomanagement im folgenden Umfang eingeführt:

- Regelmässige gemeinsame Risikobesprechungen zwischen den Produkt- und Risiko- und Compliance-Teams
- Pflege eines Inventars der identifizierten Risiken
- Jährliche unabhängige Penetrationstests durch externe Parteien
- Möglichkeit, bei Bedarf einen Penetrationstest auf Abruf durchzuführen
- Kontinuierliche Überprüfung der Codebasis auf Sicherheitslücken
- In den Entwicklungslebenszyklus integriertes Test- und Qualitätssicherungsverfahren
- Prozess für regelmässige Überprüfungen durch Dritte
- Festgelegte Richtlinie für den Umgang mit Sicherheitsvorfällen
- Festgelegte Richtlinie und definierter Prozess zur Meldung von Sicherheitsvorfällen im Einklang mit der DSGVO.
- Jährliche unabhängige interne ISO-Prüfung
- Jährliche unabhängige externe ISO-Prüfung

4. Verfahren und Richtlinie für das Schwachstellenmanagement

Unsere Verfahren für das Schwachstellenmanagement und die entsprechende Richtlinie umfassen Folgendes:

- Tägliche Scans der Codebasis (bei Codeänderung)
- Tägliche Scans unserer digitalen Zertifikate
- Kontinuierliche NIDS- und HIDS-Überwachung
- Jährliche Penetrationstests, die von einem Drittunternehmen durchgeführt werden
- Ausführung von Anti-Malware auf lokalen Endpunkten und cloudbasierten virtuellen Rechnern
- Regelmässig geplantes DAST und ASM
- Risikomanagementprozess zur Priorisierung und Behebung bekannter Schwachstellen
- Tool zum kontinuierlichen Scannen der Bibliotheken von Drittanbietern auf bekannte Sicherheitslücken

***