BEEKEEPER

BEEKEEPER
VERTRAG ZUR AUFTRAGSVERARBEITUNG »AVV«

Zwischen

Beekeeper AG
Hönggerstrasse 65
8037 Zürich
Schweiz

(Beekeeper AG als „Auftragsverarbeiter“)

Und

(als „Verantwortlicher“, falls auf Seite 1 nicht anders definiert)

Dieser **Vertrag zur Auftragsverarbeitung (»AVV«)** (DSGVO - Artikel. 28) sieht vor, dass die Parteien eine Vereinbarung über die Rollen und Verantwortlichkeiten im Rahmen der aufgeführten **Grundsätze** treffen, die zwischen dem **Auftragsverarbeiter** (Beekeeper AG, Hönggerstrasse 65, 8037 Zürich, Schweiz) gemäß der Definition der DSGVO Art. 4 (8) und dem DSGVO Art. 4 (7) definierten **Verantwortlichen**:

Dieser AVV regelt im Folgenden:

1. Bereitstellung eines AVV gemäß Artikel. 28 (3) der EU Datenschutz-Grundverordnung **(DSGVO (EU) 2016-679)** und unter der Vorschrift von Art. 6 für rechtmäßige Verarbeitung;

2. Die personenbezogenen und sonstigen Daten dürfen nur zu dokumentierten Anweisungen des Verantwortlichen verarbeitet werden, einschließlich der Beschränkung des Zugriffs durch Dritte, die diesen AVV nicht unterzeichnet haben; oder die Weitergabe personenbezogener Daten an Drittländer oder internationale Organisationen, sofern dies nicht durch das Recht der Schweiz, der EU oder eines vereinbarten Gerichtsstandes, dem der Auftragsverarbeiter unterliegt, legitimiert/erlaubt ist;

3. Der Auftragsverarbeiter wird alle geeigneten technischen und organisatorischen Maßnahmen ergreifen, einschließlich Daten-Verletzungs-Management und Benachrichtigung;

4. Transparenz bei der Verwendung aller Unterverarbeiter und Drittunternehmen gegenüber dem Verantwortlichen zu erreichen;

5. Der Auftragsverarbeiter wird seinen Unterverarbeitern die Datenschutzpflichten auferlegen, welche im Vertrag über Abonnement der Beekeeper Software-as-a-Service (oder dem Rechtsakt) zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind;

6. Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen unterstützen, soweit dies möglich ist, um die Erfüllung der Verpflichtung des Verantwortlichen sicherzustellen, auf die Anfragen von betroffenen Personen, die ihre Rechte ausüben, zu antworten;

7. Der Auftragsverarbeiter wird den Verantwortlichen dabei unterstützen, die Einhaltung seiner Sicherheits- und bestimmter anderer Verpflichtungen zu gewährleisten, wobei die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen zu berücksichtigen sind;

8. Der Auftragsverarbeiter wird nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen und anderen Daten an den Verantwortlichen nach Wahl des Verantwortlichen entweder löschen oder zurückgeben und die vorhandenen Kopien löschen, sofern nicht der schweizerische, EU- oder anderweitig vereinbarte Gerichtsstand eine Verpflichtung zur Speicherung der personenbezogenen Daten vorschreibt;

9. Der Auftragsverarbeiter wird dem Verantwortlichen alle Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung seiner Verpflichtungen erforderlich sind und Inspektionen/Audits im Auftrag vom Verantwortlichen zulassen sowie mit dem Verantwortlichen (oder dem vom Verantwortlichen gewählten Prüfer/Auditor) kooperieren.

Präambel

Dieser AVV konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag über Abonnement der Beekeeper Software-as-a-Service (nachfolgend »**Vertrag**«) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiter oder Beauftragte, personenbezogene Daten (»Daten«) des Verantwortlichen verarbeiten (nachfolgend »Datenverarbeitung«).

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Datenverarbeitung. Die Datenverarbeitung umfasst jegliche Daten, welche in **Anhang 1** dieses AVV gelistet sind, ist aber nicht darauf beschränkt.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragsverarbeiter handelt ausschließlich nach dokumentierten Anweisungen oder Servicevereinbarungen des Verantwortlichen. Der Auftragsverarbeiter stellt sicher, dass die anvertrauten Unternehmensdaten nicht für andere Zwecke verwendet oder auf andere Form als in den Anweisungen des Verantwortlichen angegeben verarbeitet werden, einschließlich der Übermittlung von Unternehmensdaten an ein Drittland oder eine internationale Organisation.

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

3. Der Auftragsverarbeiter verarbeitet die Unternehmensdaten jederzeit in Übereinstimmung mit den geltenden Gesetzen. Wenn der Auftragsverarbeiter der Ansicht ist, dass eine Anweisung gegen diese Gesetze verstößt, informiert er den Verantwortlichen unverzüglich darüber. Dies gilt jedoch nicht, falls das fragliche Gesetz eine solche Meldung aus Gründen des wesentlichen öffentlichen Interesses verbietet.

4. Der Auftragsverarbeiter darf die Unternehmensdaten nicht für einen anderen als den angegebenen Zweck verarbeiten, es sei denn, der Auftragsverarbeiter ist dazu gemäß der schweizerischen Datenschutzbehörde, der DSGVO oder der vereinbarten Datenverarbeitungs-Gerichtsbarkeit verpflichtet. In jenem Fall wird der Auftragsverarbeiter den Verantwortlichen **vor der Verarbeitung** über eine solche Verpflichtung informieren.

§ 3 Pflichten des Auftragsverarbeiters

1. Für die Erfüllung der Pflichten in Bezug auf diesen AVV bestellt der Auftragsverarbeiter nur solche Mitarbeiter, die über alle relevanten Datenschutzpflichten informiert wurden und zur Einhaltung des Datenschutzgeheimnisses vor der Erfüllung ihrer Aufgaben gemäß dem schweizerischen Datenschutzgesetz und der DSGVO der EU zur Vertraulichkeit verpflichtet wurden. Die Mitarbeiter müssen ausreichend geschult sein, um ihren datenschutzrechtlichen und vertraglichen Verpflichtungen nachkommen zu können. Der Auftragsverarbeiter stellt ein angemessenes Ausbildungsniveau durch geeignete Kontrollen sicher. Der Auftragsverarbeiter muss zusätzliche Mittel einsetzen, z. B. Hintergrundüberprüfungen der jeweiligen Mitarbeiter, wenn dies als angemessene Maßnahme zur Minderung des dem Verantwortlichen auferlegten operationellen Risikos angesehen wird.

2. Außer wenn ausdrücklich gemäß Artikel 28 (3)(a) der DSGVO erlaubt, verarbeitet der Auftragsverarbeiter die Daten der betroffenen Personen nur im Rahmen der Leistungsbeschreibung und der Anweisungen, die der Verantwortliche im Rahmen des Vertrages oder dieser AVV erteilt hat. Wenn der Auftragsverarbeiter der Ansicht ist, dass eine Anweisung gegen geltendes Recht verstoßen würde, muss der Auftragsverarbeiter den Verantwortlichen unverzüglich davon in Kenntnis setzen. Der Auftragsverarbeiter ist berechtigt, die Leistung aufgrund einer solchen Anweisung auszusetzen, bis der Verantwortliche diese Anweisung bestätigt oder ändert.

3. Der Auftragsverarbeiter 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 Verantwortlichen treffen, die den Anforderungen der DSGVO (Art. 32) genügen. 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.

4. Der Auftragsverarbeiter behält sich das Recht vor, die durchgeführten Maßnahmen zum angemessenen Schutz der Daten zu ändern, vorausgesetzt, das Sicherheitsniveau wird nicht weniger als die ursprünglich vereinbarte Sicherheit sein.

5. Der Auftragsverarbeiter unterstützt den Verantwortlichen, soweit dies zwischen den Parteien vereinbart ist und soweit möglich für den Auftragsverarbeiter, bei der Erfüllung der in Kapitel III der DSGVO dargelegten Anforderungen und Ansprüche der betroffenen Personen und bei der Erfüllung der in den Artikeln 33 bis 36 aufgeführten Verpflichtungen der DSGVO.

6. Der Auftragsverarbeiter garantiert, dass allen Mitarbeitern, die an der Vertragsabwicklung der Unternehmensdaten beteiligt sind, und anderen Personen, die im Rahmen der Verantwortlichkeit des Auftragsverarbeiters an der Vertragsabwicklung beteiligt sind, die Datenverarbeitung außerhalb des Anwendungsbereichs der Anweisungen untersagt ist. Des Weiteren gewährleistet der Auftragsverarbeiter, dass jede Person, die zur Datenverarbeitung im Auftrag des Verantwortlichen berechtigt ist, eine Geheimhaltungsverpflichtung eingegangen ist oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegt. Alle diese Geheimhaltungspflichten bleiben auch nach Beendigung oder Ablauf der Vertragsabwicklung erhalten.

7. Der Auftragsverarbeiter muss die verantwortliche Stelle unverzüglich benachrichtigen, wenn er Kenntnis von Verstößen gegen den Schutz personenbezogener Daten im Verantwortungsbereich des Auftragsverarbeiters erhält.

8. Der Auftragsverarbeiter muss die erforderlichen Maßnahmen ergreifen, um Daten zu schützen und mögliche negative Folgen für die betroffene Person zu mildern. Der Auftragsverarbeiter wird diese Bemühungen unverzüglich mit dem Verantwortlichen abstimmen.

9. Der Auftragsverarbeiter benennt dem Verantwortlichen den Ansprechpartner für im Rahmen des Vertrages und dieser AVV anfallende Datenschutzfragen.

10. Der Auftragsverarbeiter gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

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

12. Der Auftragsverarbeiter muss, wenn zum Zeitpunkt der Kündigung durch den Verantwortlichen nicht schriftlich etwas anderes verlangt wird, bei der Kündigung des Vertrages in Übereinstimmung mit der **Laufzeit- und Kündigungsklausel** des Vertrags handeln.

13. Der Verantwortliche trägt die zusätzlichen Kosten, die durch abweichende Anforderungen bei der Rückgabe oder Löschung von Daten entstehen.

14. Der Auftragsverarbeiter führt Aufzeichnungen über alle Kategorien von Verarbeitungstätigkeiten, die im Auftrag des Verantwortlichen ausgeführt werden. Das Protokoll muss Folgendes enthalten:

    - Name und Kontaktinformationen des jeweiligen Auftragsverarbeiter, eines Unterauftragsverarbeiters des Vetrages (Vertrag über Abonnement der Beekeeper Software-as-a-Service), des Verantwortlichen, des Datenschutzbeauftragten und ggf. des Vertreters des Auftragsverarbeiters.

    - Die Kategorien der Verarbeitung, die vom Auftragsverarbeiters oder einem Unterauftragsverarbeiters im Auftrag des Verantwortlichen durchgeführt werden.

    - Allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die der Auftragsverarbeiter zum Schutz der Unternehmensdaten getroffen hat, vgl. Art. 32(1) der DSGVO.

15. Die Liste muss schriftlich, auch in elektronischer Form, vorliegen. Auf Verlangen des Verantwortlichen stellt der Auftragsverarbeiter die Liste jederzeit zur Verfügung.

16. Erfolgt die Verarbeitung der Unternehmensdaten beim Auftragsverarbeiter ganz oder teilweise in den Heimbüros, so hat der Auftragsverarbeiter Richtlinien für die Verarbeitung der Unternehmensdaten durch das Personal in den Heimbüros festzulegen. Die Richtlinien sind dem Verantwortlichen auf Anfrage vorzulegen.

17. Der Auftragsverarbeiter nimmt an etwaigen Gesprächen mit dem Verantwortlichen und / oder der Datenschutzbehörde teil und berücksichtigt in gutem Glauben Empfehlungen und / oder Verbesserungshinweise usw. des Verantwortlichen und / oder der Datenschutzbehörde bezüglich der Verarbeitung von Daten des Verantwortlichen.

18. Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich informieren, wenn die Datenschutzbehörde den Auftragsverarbeiter bezüglich der von der AVV abgedeckten Unterstützung oder Dienstleistungen kontaktiert.

19. Der Auftragsverarbeiter verpflichtet sich ferner, den Verantwortlichen unverzüglich über Folgendes zu informieren:

    - Jeder Antrag einer Behörde auf Übertragung von Unternehmensdaten, die unter den Handelsvertrag fallen, sofern nicht die Benachrichtigung des Verantwortlichen gesetzlich verboten ist, z.B. gemäß Regeln, die sicherstellen sollen, dass Ermittlungen, die von einer Strafverfolgungsbehörde durchgeführt werden, nicht offengelegt werden.

    - Alle Zugangsanfragen werden direkt von der betroffenen Person oder von einer anderen Partei erhalten.

§ 4 Pflichten des Verantwortlichen

1. Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2. Der Verantwortliche muss dem Auftragsverarbeiter den Ansprechpartner für alle Fragen im Zusammenhang mit dem Datenschutz mitteilen, die sich aus oder im Zusammenhang mit der Vereinbarung in **Anhang 1** dieses AVV ergeben.

3. Im Hinblick auf die Einhaltung der in **Anhang 2** dieses AVV aufgeführten Schutzmaßnahmen und Sicherheitsvorkehrungen verpflichtet sich der Auftragsverarbeiter, ein Informationssicherheits-Managementsystem gemäß den Kontrollzielen von ISO 27001:2013 und dessen überprüfte Wirksamkeit aufrechtzuerhalten. Die Parteien verweisen auf Verlangen auf die bereits ausgestellten und verfügbaren Zertifizierungen als Nachweis der entsprechenden Garantien. Der Verantwortliche ist mit den vom Auftragsverarbeiter beschriebenen technischen und organisatorischen Maßnahmen eines ISMS vertraut, und es liegt in der Verantwortung des Verantwortlichen, dass diese Maßnahmen ein dem Risiko angemessenes Sicherheitsniveau gewährleisten.

§ 5 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragsverarbeiter, wird der Auftragsverarbeiter die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung an den Verantwortlichen nach Angaben der betroffenen Person möglich ist.

2. Der Auftragsverarbeiter leitet den Antrag der betroffenen Person unverzüglich an den Verantwortlichen weiter.

3. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart.

4. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Verantwortlichen nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1. Der Auftragsverarbeiter weist dem Verantwortlichen die Einhaltung der in diesem AVV niedergelegten Pflichten mit geeigneten Mitteln nach.

2. Können auch konkrete Arten von Nachweisen genannt werden bzw. zum Nachweis der Einhaltung der vereinbarten Pflichten, kann der Auftragsverarbeiter, dem Verantwortlichen folgende Informationen zur Verfügung vorlegen:

    - Durchführung eines Selbst Audits
    - unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung
    - Zertifikat zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001)
    - Jährlicher Penetration Test-Bericht, der von einem externen Unternehmen durchgeführt wurde
    - Jegliche technischen und/oder organisatorischen Informationen, die vom Verantwortlichen als notwendig erachtet werden, **mit Ausnahme** von Informationen, die potenziell, auch entfernt, die Sicherheit und/oder Vertraulichkeit eines anderen Kunden oder Lieferanten des Auftragsverarbeiters beeinträchtigen können.

§ 7 Recht auf Inspektion und Prüfung (Audits)

1. Der Verantwortliche hat das Recht, die vom Auftragsverarbeiter ergriffenen technischen und organisatorischen Maßnahmen jederzeit zu überwachen.

2. Sollten im Einzelfall, um technischen und organisatorischen Maßnahmen zu überprüfen, Inspektionen durch den Verantwortlichen oder einen von diesem beauftragten Prüfer/Auditor erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Diese Inspektionen erfordern eine schriftliche Bestätigung des Auftragsverarbeiters.

3. Der Auftragsverarbeiter darf Inspektionen von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

4. Sollte der durch den Verantwortlichen beauftragte Prüfer/Auditor in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.

5. Der Auftragsverarbeiter ist berechtigt, eine Vergütung für die Unterstützung des Auftragsverarbeiters bei der Durchführung von Inspektionen zu verlangen. Sofern der betriebliche Ablauf nicht gestört wird, wird bei einer ersten Prüfung auf eine Vergütung verzichtet.

6. Der Zeit- und Arbeitsaufwand des Auftragsverarbeiters für solche Inspektionen ist auf einen Besuch pro Kalenderjahr, höchstens drei Tage, begrenzt, sofern nichts anderes vereinbart ist.

7. Der Verantwortliche ist für alle betriebsfremden anfallenden Kosten verantwortlich, welche dem Auftragsverarbeiter für eine solche Prüfung oder Überprüfung entstehen.

8. Der physische Zugriff auf die Rechenzentrumsstandorte des Auftragsverarbeiters ist von einer solchen Prüfung oder Überprüfung ausgeschlossen.

9. Wenn eine Datenschutzaufsichtsbehörde oder eine andere für den Verantwortlichen gesetzlich zuständige Aufsichtsbehörde eine Inspektion durchführt, die vorstehenden Absätze 1 bis 6 gelten entsprechend. Die Vollstreckung einer Geheimhaltungsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde beruflichen oder gesetzlichen Geheimhaltungspflichten unterliegt, deren Verletzung nach dem anwendbaren Strafgesetzbuch sanktionierbar ist.

§ 8 Subunternehmer/Unterauftragsverarbeiter (weitere Auftragsverarbeiter)

1. Der Auftragsverarbeiter kann im Namen des Verantwortlichen Unterauftragsverarbeiter als weitere Auftragsverarbeiter einsetzen.

2. Unterauftragsverarbeiter sind nur jene in **Anhang 1** dieses AVV angegebenen oder solche, welche vom Verantwortlichen vorab genehmigt worden sind.

3. Ein Unterauftragsverarbeiter-Verhältnis unterliegt der Zustimmung des Auftragsverarbeiter, der den Unterauftragsverarbeiter mit der in dem Vertrag bestimmten Leistung ganz oder teilweise beauftragt.

4. Der Auftragsverarbeiter schließt mit diesen Unterauftragsverarbeitern die vertraglichen Instrumente ab, die zur Gewährleistung eines angemessenen Datenschutz- und Informationssicherheitsniveaus und im Einklang mit den anwendbaren Datenschutzbestimmungen erforderlich sind.

5. Der Auftragsverarbeiter führt die Software-as-a-Service-Leistung in der Vereinbarung durch, wobei er Dienstanbieter von Drittanbietern verwendet, wie im Beekeeper 3rd Party Use Statement aufgeführt.

6. Gemäß der DSGVO Art. 4.10 „Dritter“ bezeichnet eine natürliche oder juristische Person, Behörde, Agentur oder Einrichtung, die nicht der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und Personen unterliegt, die unter der direkten Aufsicht des Verantwortlichen oder des Auftragsverarbeiters befugt sind, personenbezogene Daten zu verarbeiten.

7. Abgesehen von den Infrastructure as a Service (IaaS) Providern, welche für Data Center-Dienste verwendet werden, und andere in **Anhang 1** dieses AVV angegebene Unterauftragsverarbeiter, werden neue oder Änderungen von Drittanbietern, welche im 3rd Party Use Statement aufgeführt sind, nicht als Änderung oder neuer Unterauftragsverarbeiter angesehen und deren Verwendung obliegt deshalb nicht der Zustimmung, Akzeptanz oder Meldung gegenüber des Verantwortlichen.

8. Der Auftragsverarbeiter ist dafür verantwortlich, sicherzustellen, dass die Nutzung von Drittanbietern rechtmäßig und in der Definition der anwendbaren Anforderungen und des Rahmens der vereinbarten Datenschutzgesetze erfolgt.

9. Der Auftragsverarbeiter muss das Einverständnis des Verantwortlichen einholen, bevor neue Unterauftragsverarbeiter eingesetzt oder bestehende ersetzt werden, gemäß DSGVO-Art. 7.

10. Der Verantwortliche ist berechtigt, einer Änderung der schriftlichen Benachrichtigung des Auftragsverarbeiters aus wesentlich wichtigen Gründen im Zusammenhang mit den gesetzlichen Datenschutzbestimmungen oder aufgrund des Unternehmensrisikos aufgrund von Wettbewerbsnachteilen zu widersprechen.

11. Der Auftragsverarbeiter muss dem Verantwortlichen sechs (6) Monate vor dem Einsatz des neuen oder des Ersatz-Unterauftragsverarbeiter benachrichtigen. Die Benachrichtigung muss schriftlich erfolgen.

12. Widerspricht der Verantwortliche einer solchen Änderung nicht innerhalb dieser Frist, gilt der Verantwortliche als mit dieser Änderung einverstanden.

13. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, sind sowohl der Verantwortliche als auch der Auftragsverarbeiter berechtigt, den Vertrag und diesen AVV zu kündigen, um einen neuen oder Ersatz-Unterauftragsverarbeiter zu verwenden.

14. Erteilt der Auftragsverarbeiter Aufträge an Unterauftragsverarbeiter, so obliegt es dem Auftragsverarbeiter, seine datenschutzrechtlichen Pflichten aus diesem AVV dem Unterauftragsverarbeiter zu übertragen.

15. Sämtliche Kosten für den Abschluss einer Vereinbarung mit einem Unterauftragsverarbeiter oder einem Dritten, einschließlich der Kosten im Zusammenhang mit dem Abschluss von Unterprozessvereinbarungen, gehen zu Lasten des Auftragsverarbeiters und sind für den Verantwortlichen nicht von Belang.

16. Die Tatsache, dass der Verantwortliche dem Abschluss eines Vertrages mit einem anderen Unterauftragsverarbeiter durch den Auftragsverarbeiter zugestimmt hat, hat keinen Einfluss auf die Verpflichtung des Auftragsverarbeiters, diesen AVV einzuhalten.

§ 9 Verletzungs-Management und Benachrichtigung

1. Gemäß der DSGVO Art. 4 (12) „Verletzung des Schutzes personenbezogener Daten" bezeichnet eine Sicherheitsverletzung, die zu einer versehentlichen oder rechtswidrigen Zerstörung, zum Verlust, zur Änderung, zur unberechtigten Offenlegung oder zum Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.

2. Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich schriftlich über jeden Verstoß gegen personenbezogene Daten bei der Verarbeitung von persönlichen ODER Unternehmensdaten, wie in diesem AVV angegeben, informieren.

3. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle Informationen zur Verfügung zu stellen, die zur Erfüllung der Verpflichtungen des Verantwortlichen gemäß dem schweizerischen Datenschutzgesetz (bzw. Der geltende Gerichtsbarkeit) bezüglich der Verarbeitung personenbezogener Daten und der DSGVO oder den sonstigen Bestimmungen zum Schutz personenbezogener Daten erforderlich sind.

4. Der Auftragsverarbeiter muss dem Verantwortlichen dann unverzüglich, spätestens jedoch 72 Stunden nach dem Verstoß gegen personenbezogene Daten, Bericht erstatten.

5. Gemäß den in der DSGVO Artikel 33, 34 umrissenen Informationsanforderungen muss der Auftragsverarbeiter den Verantwortlichen über den Hintergrund der Sicherheitsverletzung und deren Ausmaß sowie Informationen über Initiativen zur Abwehr zukünftiger Sicherheitsverletzungen informieren.

Für Klarheit und Transparenz:

Um etwaige Annahmen zu streichen - ein meldepflichtiger Verstoß ist ein Verstoß, der in der DSGVO festgelegt ist. 34 (1) „Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung."

- Im Falle einer Verletzung der Datensicherheit, bei dem die persönlichen ODER Firmendaten betroffen sind, meldet dies der Auftragsverarbeiter dem Verantwortlichen unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, gemäß den Anforderungen in den Artikeln 33 und 34 der DSGVO (Datenschutzverordnung (EU) 2016/679).

§10 Technische und organisatorische Maßnahmen

1. Um den Schutz der Unternehmensdaten zu gewährleisten und die Gesetze und Vorschriften für personenbezogene Daten einzuhalten, ergreift der Auftragsverarbeiter die technischen und organisatorischen Maßnahmen gemäß Art. 32 der DSGVO.

2. Der Auftragsverarbeiter muss die Unternehmensdaten mit den erforderlichen technischen und organisatorischen Maßnahmen (unter anderem in Bezug auf Speicherung, Datenverarbeitung, Netzwerkzugriff, Übertragung, Eingabe, Auftrag und Verfügbarkeitskontrolle) implementieren und somit sichern. Zu den Schutzmaßnahmen zählen die Verwendung modernster Software, Computer und Verschlüsselungsverfahren sowie die Verwendung angemessener Zugriffskontrollen für die Authentifizierung und Autorisierung (z.B. Zwei-Faktor-Authentifizierung und Vier-Augen-Kontrolle für Autorisierungsprozesse), Passwortverfahren, Protokollierung und Prozessdokumentation und Implementierung eines Datensicherheitskonzeptes gemäß den im Security White Paper des Auftragsverarbeiters beschriebenen Maßnahmen.

3. Die getroffenen Maßnahmen müssen zum Schutz der spezifischen Unternehmensdaten angemessen sein und vor versehentlicher oder rechtswidriger Zerstörung, Verlust oder Veränderung sowie vor unbefugter Offenlegung, Missbrauch oder anderweitiger, gegen geltendes Recht verstoßender Verarbeitung (einschließlich, aber nicht beschränkt auf das schweizerische Datenschutzgesetz über die Verarbeitung personenbezogener Daten sowie DSGVO) zu schützen. Dies gilt auch dann, wenn die Verarbeitung der Firmendaten ganz oder teilweise in den Home Offices erfolgt.

4. Wenn der Auftragsverarbeiter in einem anderen EU-Mitgliedstaat niedergelassen ist, muss der Auftragsverarbeiter sowohl die Sicherheitsbestimmungen einhalten, welche am Betriebsort des Verantwortlichen für das Unternehmen gelten, als auch diejenigen, in dem Mitgliedstaat oder der Gerichtsbarkeit des Auftragsverarbeiters festgelegt sind. Bei der Übertragung der Unternehmensdaten werden elektronisch übermittelte oder zum Download zur Verfügung gestellte Daten vor unberechtigtem Zugriff geschützt.

§11 Übertragung von Unternehmensdaten

Der Auftragsverarbeiter darf die Übertragung von Unternehmensdaten in Länder außerhalb der vereinbarten und mitgeteilten Gerichtsbarkeit/en in dem Vertrag und diesem AVV mit dem Verantwortlichen nicht übertragen oder autorisieren.

§12 Geheimhaltungspflicht

1. Der Verantwortliche und das Personal des Verantwortlichen müssen die vorbehaltlose Vertraulichkeit in Bezug auf die Verarbeitung der Unternehmensdaten einhalten. Der Auftragsverarbeiter und das Personal des Auftragsverarbeiters sind daher nur berechtigt, die Unternehmensdaten im Rahmen der Erfüllung des Vertrages einschließlich dieses AVV zu verarbeiten.

2. Der Auftragsverarbeiter gewährleistet, dass das Personal des Auftragsverarbeiter und alle anderen Unterauftragsverarbeiter und das Personal dieses anderen Datenverarbeiters, die zur Verarbeitung von Firmendaten gemäß diesem AVV befugt sind, hinsichtlich der Firmendaten, die ihnen bekannt werden, der Geheimhaltungspflicht unterliegen im Zusammenhang mit der Vertragserfüllung.

§13 Rückgabe und Löschung von Unternehmensdaten bei Stornierung und Kündigung

Vorbehaltlich der **Laufzeit- und Kündigungsklausel** des Vertrags oder nach schriftlicher Anweisung des Verantwortlichen und gemäß den einschlägigen gesetzlichen Bestimmungen wird der Auftragsverarbeiter die Korrektur, Löschung und Sperrung der im Auftrag des Verantwortlichen verarbeiteten Unternehmensdaten ermöglichen, bis diese Unternehmensdaten letztendlich gemäß dem Vertrag gelöscht werden.

§14 Dauer

1. Der AVV tritt mit seiner Unterzeichnung in Kraft und bleibt so lange in Kraft, wie der Auftragsverarbeiter im Auftrag des Verantwortlichen Daten verarbeitet oder bis der Vertrag ausläuft oder endet, je nachdem was später eintrifft.

2. Bei Ablauf oder Kündigung des AVV erbringt der Auftragsverarbeiter, ungeachtet der rechtlichen Gründe der Kündigung, die erforderlichen Dienstleistungen gemäß Ziffer 3 dieses AVV.

§15 Informationspflicht, zwingende Schriftform, Rechtswahl

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

2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – 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 dieses AVV handelt.

3. Bei etwaigen Widersprüchen gehen Regelungen dieses AVV den Regelungen des Vertrages vor. Sollten einzelne Teile dieses AVV unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

4. Das anwendbare Recht und der Gerichtsstand für diesen AVV entsprechen dem Vertrag.

§16 Haftung und Schadensersatz

Haftung und Schadensersatz für diesen AVV ist in erster Linie das, was von einem Gericht festgelegt werden kann und in der Abwesenheit oder Vereinbarung eines Ausschlusses der ersten Instanz im Einklang mit der im Vertrag festgelegten Haftung und Schadensersatz.

§17 Vorrang

Im Falle einer Abweichung zwischen den Bedingungen dieses AVV und etwaigen anderen, schriftlichen oder mündlichen, Handelsvereinbarungen zwischen den Parteien, einschließlich des Vertrages über das Abonnement der Beekeeper Software-as-a-Service, haben die Anforderungen, die im Schweizer Bundesgesetz über den Datenschutz für die in der Schweiz verarbeiteten Daten des Datenverantwortlichen in der jeweils gültigen Fassung gelten sowie die Anforderungen der DSGVO der EU für alle anderen Gerichtsbarkeiten Vorrang.

§18 Gegenstück und elektronische Unterschriften

Der Vertrag zur Auftragsverarbeitung wird in zwei Originalausfertigungen unterzeichnet, von denen die Vertragsparteien jeweils eine erhalten. Dieser AVV kann in Form von Gegenstücken ausgeführt werden, von denen jede als Original gilt, aber alle zusammen ein und dasselbe Instrument bilden. Fotokopien, elektronische PDF- und Faksimile-Kopien dieser unterzeichneten Gegenstücke können für jeden Zweck anstelle der Originale verwendet werden. Die unten aufgeführten autorisierten Signaturen können elektronische Signaturen sein, die der örtlichen Rechtspraxis entsprechen.

Auftragsverarbeiter	**Verantwortlicher**
Firma: Beekeeper AG	Firma:
Name:	Name:
Titel:	Titel:
Ort und Datum:	Ort und Datum:
Firma: Beekeeper AG	Firma:
Name:	Name:
Titel:	Titel:
Ort und Datum:	Ort und Datum:

ANHANG 1

Beschreibung der Übermittlung und Verarbeitung

1. **Katalog [und Klassifizierung der Sensibilität] personenbezogener Daten, die übermittelt oder verarbeitet werden sollen:**

2. **Zweck(e) der Übermittlung und Verarbeitung:**

3. **Kategorien der betroffenen Personen:**

4. **Personen, die Zugriff auf personenbezogene Daten haben oder diese erhalten können:**

Unterauftragsverarbeiter (Name, Rechtsform, Sitz)	**Gerichtsbarkeit der Datenverarbeitung**	**Art der Dienstleistung**

5. Weitere nützliche Informationen (Angabe eventuell vereinbarter Definitionen):

6. Kontaktinformationen für Anfragen zum Datenschutz (Datenschutzbeauftragter):

BEEKEEPER Datenschutzbeauftragter (DPO)	**Dr. Amir Ameri**	**Tel. Nummer / email address** amir.ameri@beekeeper.io dpo@beekeeper.io

ANHANG 2

Vom Auftragsverarbeiter umgesetzte technische und organisatorische Maßnahmen

Dokumentation der technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter für die ordnungsgemäße Erfüllung der erbrachten Dienstleistung (Art. 32 DSGVO) umsetzt.

Anmerkung: Der Auftragsverarbeiter darf die technischen und organisatorischen Maßnahmen auf den neuesten Stand der Technik aktualisieren ohne das Datenschutzniveau zu senken.

Beschreibung der Maßnahmen, um ein Schutzniveau zu gewährleisten, das dem Risiko entspricht, unter anderem gegebenenfalls:

(1) Maßnahmen zur Pseudonymisierung und Verschlüsselung von personenbezogenen Daten

Da wir beim aktuellen Service- und Produktangebot keine Daten außerhalb der Produktplattform verarbeiten, auf die Speicherung von Daten begrenzt ist, nutzen wir kein Maßnahmen zur Pseudonymisierung. Wir verschlüsseln Daten, einschließlich personenbezogener Daten, soweit diese verfügbar sind, wie in unserem Security White Paper im Anhang beschrieben. Zusammengefasst, nutzen wir eine Verschlüsselung zur Speicherung der Daten auf mobilen Geräten. Unsere DB, die auf unserem VPC in der Schweiz liegt, ist verschlüsselt. In der Praxis verwenden wir nur verschlüsselte Verbindungen als Übermittlungskanäle. Bitte lesen Sie dazu unser Security White Paper.

(2) Laufende Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Systeme und Dienstleistungen:

Wir haben eine Reihe von Maßnahmen eingeführt, um die Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der angebotenen Dienstleistungen, wie unten aufgeführt, sicherzustellen:

1. Ein Information Security Management System (ISMS) zertifiziert nach den ISO 27001:2013 Kontrollzielen.

2. Verankerte Governance-Struktur für operatives Risikomanagement. Diese beinhaltet einen umfassenden Operativen Risikomanagement-Prozess, einschließlich BERI (Beekeeper Risk Inventory).

3. Zweistufige Authentifizierung für alle Mitarbeiter.

4. Lösung für einen sicheren Arbeitsplatz mit verschlüsselten Notebooks und installierter Endpoint Protection (Antivirus & Anti-Malware).

5. Installation einer VPC (virtuelle private Cloud) mit Begrenzung auf eine Zuständigkeit, die vom Datenverantwortlichen gewählt wird. Alle Datenzentrum-Partner sind, neben anderen Anforderungen, ISO 27001 zertifiziert.

6. Schutz der VPC-Umgebung mit einer getrennten Sicherheitsarchitektur einschließlich Border Firewalls, die vollständig von Beekeeper-Mitarbeiter kontrolliert werden. (Security White Paper)

7. Begrenzter Zugang zum Produktionsmandant für autorisierte Beekeeper-Mitarbeiter auf Grundlage der Beekeeper Information Security Policy for Customers.

8. Kein permanenter Zugang zur Produktionsumgebung, außer für die unter Punkt 6 beschriebenen Personen.

9. Governance über den Berechtigungszugriff nach dem Prinzip „Notwendigkeit zu Handeln – Notwendigkeit auf Zugriff“.

10. Zugriff des Produktionsumgebung wird durch ein Kontrollverfahren durch den eingesetzten Customer Success Manager geschützt.

11. Kontrollverfahren für den Zugriff auf Tenants für den technischen Support auf eine begrenzte Zeit (1 Stunde) mit einem von einem VPN ausgestellten Zertifikat (Notification bei Ausstellung).

12. Trennung von Zugriff auf Produktions, Staging, und Entwicklungsumgebung

13. Bereitstellung von Dashboard-Funktionalitäten für die komplette Benutzerverwaltung vor Ort durch den Datenverantwortlichen.

14. Bereitstellung einer direkten Schnittstelle zu SSO oder AD oder SFTP-Lösungen für die Zugriffsverwaltung für autorisierte Benutzer. (falls durch den Datenverantwortlichen bereitgestellt)

15. Verwendung eines Push-Prinzips bei der Beauftragung von Dienstleistungen durch eine Drittpartei.

16. Festgelegte Richtlinie über die Bewertung von Drittparteien (angefügt)

17. Festgelegtes und kontrolliertes Änderungsmanagement basierend auf Absender/Prüfer/Genehmiger und Umsetzer. Hohes Maß der Automatisierung in einer Microservices-Umgebung.

18. Verschlüsselte TLS 1.2-Kommunikation mit täglicher Verifizierung des Zertifikats

19. Angemessene Protokollierung des Zugangs zur Beekeeper-Produktionsumgebung

20. Von Risk & Compliance festgelegte Kontrollmaßnahmen

21. Risikomanagement Governance im folgenden Umfang:

    a. Wöchentliche und vierteljährliche Risiko-Treffen mit Engineering und Risk & Compliance

    b. Beibehaltung eines Risikoprofils durch Eingabe aller erkannten operativen Risiken in BERI

    c. Jährliche Penetrationtests durch eine externe Firma

    d. Penetrationtests auf Nachfrage von Kunden

    e. Im Änderungsmanagement integrierte automatisierte Sicherheitsrisiko-Scans

    f. Jährliche Risikobewertung von Drittparteien (falls zutreffend)

22. Verwendung einer angeboten Datensicherung- und Wiederherstellungslösung mit hoher Ausfallsicherheit

23. Datenverantwortlicher hat die Möglichkeit zur Online-Überwachung der Dienstleistungsverfügbarkeit und der Abonnements (status.beekeeper.io).

24. Vertraglich gebundene Verpflichtung zur Dienstleistungsverfügbarkeit von 99,9 %

(3) Maßnahmen zur rechtzeitigen Wiederherstellung der Verfügbarkeit von und des Zugriffs auf personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls.

Als Unternehmen spielt Beekeeper vierteljährlich ein Szenario im Hinblick auf Betriebskontinuität und Notfallwiederherstellung durch, wie in der BCP/DR-Richtlinie für Beekeeper festgelegt.

(4) Ein Verfahren zur regelmäßigen Prüfung, Bewertung und Beurteilung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Risikomanagement Governance im folgenden Umfang:

1. Wöchentliche und vierteljährliche Risiko-Treffen mit Engineering und Risk & Compliance

2. Beibehaltung eines Risikoprofils durch Eingabe aller erkannten operativen Risiken in BERI (Beekeeper Risk Inventory)

3. Jährliche Penetrationtests durch eine externe Firma

4. Penetrationtests auf Nachfrage von Kunden

5. Kontinuierliche Sicherheitsrisiko-Scans der Codebasis

6. Im Änderungsmanagement integrierte Tests und Qualitätssicherung

7. Jährliche Risikobewertung von Drittparteien falls gemäß der Beekeeper Richtlinie über die Bewertung von Drittparteien zutreffend

8. Festgelegte Richtlinie zu Sicherheitsvorfällen und Krisenmanagement

9. Festgelegte Richtlinie zur Benachrichtigung von Sichherheitsvorfällen nach DSGVO (Art. 33 und 34)

10. Interne Bewertungen nach ISO 27001 Kontrollziele von einem ISO 27001 zertifizierten internen Überprüfer.

***