Version: 19. Juni 2023

Auftragsverarbeitungs-vereinbarung

1 Verarbeitungstätigkeiten und Definitionen

(1) Diese Auftragsverarbeitungsvereinbarung („**AVV**“) ergänzt den in **Appendix 1** genannten Vertrag und gilt für jegliche Verarbeitung personenbezogener Daten, bei der der in **Appendix 1** genannte Auftragnehmer („**Auftragsverarbeiter**“), seine Angestellten oder Unterauftragnehmer mit personenbezogenen Daten in Berührung kommen, die vom Auftragsverarbeiter im Auftrag des in **Appendix 1** genannten Kunden („**Verantwortlicher**“) als Teil der Erbringung von Services i.S.v. **Appendix 1** gemäß dem dort genannten Vertrag verarbeitet werden. Der Gegenstand, die Dauer, die Art und die Zwecke der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen sind in **Appendix 1** zu dieser AVV aufgeführt und variieren ggf. bei einzelnen erbrachten Services.

Begriffe, die in dieser AVV verwendet werden und in der Datenschutz-Grundverordnung (EU 2016/679 – „**DSGVO**“), nicht jedoch in dieser AVV oder an anderer Stelle im Vertrag, definiert sind, haben die in der DSGVO festgelegte Bedeutung.

2 Verarbeitung im Auftrag des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen nur im Rahmen des Vertrages gemäß den dokumentierten Weisungen des Verantwortlichen, sofern der Auftragsverarbeiter nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist.

(2) Zusätzliche Weisungen müssen schriftlich oder in elektronischer Form (Textform) erteilt werden. Zusätzliche mündliche Weisungen müssen vom Verantwortlichen umgehend schriftlich oder in Textform bestätigt werden.

(3) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung anwendbare Datenschutzgesetze verletzt, wird er dies dem Verantwortlichen unverzüglich mitteilen und ist zudem berechtigt, die Ausführung der betreffenden Weisungen auszusetzen, bis der Verantwortliche diese bestätigt oder ändert.

3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter wird die in den Anwendungsbereich der AVV fallenden personenbezogenen Daten des Verantwortlichen nicht für andere Zwecke als die im Vertrag beschriebenen und nur zur Erfüllung seiner Pflichten aus dem Vertrag nutzen.

(2) Jederzeit während der Verarbeitung wird der Auftragsverarbeiter personenbezogene Daten im Anwendungsbereich dieser AVV berichtigen, löschen oder sperren, wenn der Verantwortliche eine entsprechende Weisung erteilt.

(3) Das Personal des Auftragsverarbeiters, das mit der Durchführung der Verarbeitungstätigkeiten gemäß dieser AVV befasst ist, ist zur Vertraulichkeit zu verpflichten, soweit es nicht bereits einer entsprechenden gesetzlichen Vertraulichkeitspflicht unterliegt.

(4) Der Auftragsverarbeiter wird dem Verantwortlichen einen Ansprechpartner für alle Fragen bezüglich des Datenschutzes im Rahmen des Vertrages benennen.

(5) Der Auftragsverarbeiter wird seine internen Prozesse und die technischen und organisatorischen Maßnahmen regelmäßig überwachen, um sicherzustellen, dass die in seinem Verantwortungsbereich liegende Verarbeitung in Übereinstimmung mit den anwendbaren Datenschutzgesetzen erfolgt.

(6) Der Auftragsverarbeiter wird den Verantwortlichen in angemessener Weise bei der Erfüllung seiner Pflichten gemäß Art. 32 bis 36 DSGVO oder entsprechenden Pflichten gemäß sonstigen anwendbaren Datenschutzgesetzen unterstützen.

(7) Der Auftragsverarbeiter darf personenbezogene Daten sowohl in Mitgliedstaaten der Europäischen Union ("**EU**") oder des Europäischen Wirtschaftsraums ("**EWR**") als auch außerhalb dieser verarbeiten. Jede Übermittlung personenbezogener Daten in einen Staat, der kein Mitgliedstaat der EU oder des EWR ist, darf nur erfolgen, wenn die speziellen Bedingungen der Art. 44 ff. DSGVO oder die entsprechenden Anforderungen anderer anwendbarer Datenschutzgesetze erfüllt sind.

4 Pflichten des Verantwortlichen

(1) Der Verantwortliche wird die Einhaltung der gesetzlichen Bestimmungen der anwendbaren Datenschutzgesetze sicherstellen, insbesondere im Hinblick auf die erforderliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen.

(2) Der Verantwortliche wird den Auftragsverarbeiter unverzüglich, jedoch spätestens innerhalb von achtundvierzig (48) Stunden, informieren, wenn der Verantwortliche Fehler oder Unregelmäßigkeiten bei den Verarbeitungstätigkeiten feststellt, die eine Einhaltung der anwendbaren Datenschutzgesetze beeinträchtigen.

5 Rechte der betroffenen Personen

(1) Der Auftragsverarbeiter ist nicht verpflichtet, auf Anfragen betroffener Personen direkt zu antworten, und wird die betroffenen Personen an den Verantwortlichen verweisen, wenn die von der betroffenen Person gelieferten Informationen ausreichen, um den Verantwortlichen, den die Anfrage betrifft, zu identifizieren. Das

Vorstehende gilt entsprechend, wenn eine betroffene Person den Auftragsverarbeiter auffordert, Daten zu berichtigen, zu löschen oder zu sperren.

(2) Ist der Verantwortliche verpflichtet, eine Anfrage einer betroffenen Person bezüglich der Verarbeitung personenbezogener Daten zu beantworten, wird der Auftragsverarbeiter den Verantwortlichen in angemessener Weise bei der Lieferung der verlangten Informationen unterstützen. Der Auftragsverarbeiter ist nur verpflichtet, die Informationen auf eine dokumentierte Weisung des Verantwortlichen hin zu liefern. Der Auftragsverarbeiter haftet nicht, wenn der Verantwortliche die Anfrage der betroffenen Person nicht richtig oder nicht fristgemäß beantwortet, oder wenn der Verantwortliche die Anfragen der betroffenen Person überhaupt nicht beantwortet.

(3) Wenn die betroffene Person gegen den Auftragsverarbeiter Ansprüche gemäß Art. 82 DSGVO oder entsprechenden Regelungen der sonstigen anwendbaren Datenschutzgesetze geltend macht, verpflichtet sich der Verantwortliche, den Auftragsverarbeiter bei der Verteidigung gegen solche Ansprüche in angemessener Weise zu unterstützen.

6 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen treffen und aufrechterhalten, die in **Appendix 2** zu dieser AVV dargelegt sind, welche zwischen einzelnen Services differenzieren kann.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter darf die technischen und organisatorischen Maßnahmen anpassen, vorausgesetzt, die neuen Maßnahmen unterschreiten nicht das von den festgelegten Maßnahmen gewährleistete Schutzniveau. Wesentliche Änderungen sind zu dokumentieren.

7 Mitteilung im Falle einer Verletzung des Schutzes personenbezogener Daten

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich benachrichtigen, wenn der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes personenbezogener Daten des Verantwortlichen erlangt und in zumutbarer Art und Weise verfügbare Informationen zur Verfügung stellen, die der Verantwortliche benötigt, um seinen Benachrichtigungspflichten gegenüber betroffenen Personen und/oder Meldepflichten gegenüber zuständigen Datenschutzaufsichtsbehörden nachzukommen. Der Verantwortliche weist den Auftragsverarbeiter an, alle Maßnahmen zu ergreifen, die der Auftragsverarbeiter als notwendig oder hilfreich ansieht, um die im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten zu schützen und mögliche nachteilige Auswirkungen für die betroffene Person zu minimieren.

8 Unterbeauftragung

(1) Der Auftragsverarbeiter darf ohne die vorherige gesonderte oder allgemeine schriftliche Zustimmung des Verantwortlichen die Verarbeitung personenbezogener Daten weder ganz noch teilweise an

Unterauftragsverarbeiter untervergeben. Der Verantwortliche erklärt hiermit seine gesonderte Zustimmung dazu, dass der Auftragsverarbeiter zur Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen Unterauftragsverarbeiter einsetzt, wie in **Appendix 1** zu dieser AVV geregelt, wobei diese zwischen einzelnen Services differenzieren kann. Der Verantwortliche erteilt hiermit seine allgemeine Zustimmung dazu, dass der Auftragsverarbeiter zur Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen weitere Unterauftragsverarbeiter einsetzt, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der DSGVO oder entsprechender Anforderungen sonstigen anwendbaren Datenschutzrechts erfolgt.

(2) Der Auftragsverarbeiter wird den Verantwortlichen informieren, bevor er von der allgemeinen Zustimmung zur Änderung oder Ergänzung der gemäß **Appendix 1** zu dieser AVV eingesetzten Unterauftragsverarbeiter Gebrauch macht, dabei angeben, wie ein Schweigen ausgelegt wird und damit dem Verantwortlichen Gelegenheit geben, der Änderung zu widersprechen. Der Verantwortliche wird den Auftragsverarbeiter unverzüglich schriftlich innerhalb von vierzehn (14) Tagen nach Zugang der Mitteilung des Auftragsverarbeiters informieren, wenn er den Ersatz- oder den zusätzlichen Unterauftragsverarbeiter ablehnt und darüber, aus welchen berechtigten Gründen er dies tut.

(3) Wenn der Verantwortliche nicht rechtzeitig widerspricht, gilt dies als Zustimmung zur Änderung oder Ergänzung der gemäß **Appendix 1** eingesetzten Unterauftragsverarbeiter. Wenn der Verantwortliche widerspricht, ist der Auftragsverarbeiter berechtigt, entweder diese AVV schriftlich mit einer Frist von dreißig (30) Tagen zu kündigen oder angemessene Anstrengungen zu unternehmen, um dem Verantwortlichen eine Änderung der Verarbeitungstätigkeiten vorzuschlagen, um die Verarbeitung personenbezogener Daten durch den Ersatz- oder zusätzlichen Unterauftragsverarbeiter zu vermeiden. Die vorgeschlagene Änderung darf den Verantwortlichen nicht unzumutbar belasten. Wählt der Auftragsverarbeiter die Option einer Änderung der Verarbeitungstätigkeiten und ist der Auftragsverarbeiter dann nicht in der Lage, die Änderung innerhalb einer angemessenen Frist durchzuführen, oder genehmigt der Verantwortliche die vorgeschlagene Änderung nicht, wobei die Genehmigung nicht unbillig verweigert werden darf, kann jede Partei den AVV durch schriftliche Mitteilung gegenüber der anderen Partei mit einer Frist von dreißig (30) Tagen kündigen.

(4) Beim Einsatz von Unterauftragsverarbeitern zur Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen wird der Auftragsverarbeiter die Erfüllung der folgenden Bedingungen sicherstellen:

- Der Vertrag über die Unterauftragsverarbeitung muss die zwischen dem Verantwortlichen und dem Auftragsverarbeiter in diesem AVV vereinbarten Datenschutzbestimmungen widerspiegeln.
- Der Auftragsverarbeiter ist für das Verhalten und die Leistung eines jeden genehmigten Unterauftragsverarbeiters verantwortlich und ist die einzige Anlaufstelle des Verantwortlichen bezüglich der Verarbeitung personenbezogener Daten durch den Unterauftragsverarbeiter.

9 Prüfungsrechte

(1) Auf vorherige schriftliche Anfrage wird der Auftragsverarbeiter dem Verantwortlichen bescheinigen, dass er diese AVV einhält, indem er angemessene Nachweise in Form von Ergebnissen einer Eigenprüfung, unternehmensinternen Verhaltensregeln, einschließlich eines externen Nachweises zu deren Einhaltung, Zertifikaten zu Datenschutz und/oder Informationssicherheit (z. B. ISO 27001), genehmigten Verhaltenskodizes oder anderen sachgemäßen Zertifikaten vorlegt. Der Nachweis der Umsetzung von Maßnahmen, die nicht nur für diese AVV spezifisch sind, kann in Form aktueller Testate, durch Berichte oder Auszüge aus Berichten unabhängiger Stellen (z. B. externer Prüfer, Innenrevision, Datenschutzbeauftragter,

IT-Sicherheitsabteilung oder Qualitätsprüfer) oder durch geeignete Zertifizierungen im Wege einer IT-Sicherheits- oder Datenschutzüberprüfung erbracht werden.

(2) Der Verantwortliche hat das Recht, die Einhaltung dieser AVV seitens des Auftragsverarbeiters zu prüfen, wenn der Verantwortliche aus triftigen Gründen, die dem Auftragsverarbeiter mitzuteilen sind, die Rechte gemäß Absatz 1 in einem Einzelfall als nicht ausreichend erachtet, oder wenn eine zuständige Datenschutzaufsichtsbehörde eine Prüfung verlangt. Die Prüfung darf nur während der normalen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters unter Berücksichtigung einer angemessenen Vorlaufzeit, die in keinem Fall kürzer als dreißig (30) Tage sein darf, durchgeführt werden. Der Auftragsverarbeiter kann die Prüfung davon abhängig machen, dass eine Vertraulichkeitsvereinbarung bezüglich der Daten anderer Kunden und der getroffenen technischen und organisatorischen Maßnahmen unterzeichnet wird.

(3) Der Verantwortliche darf keinen Dritten als Prüfer einsetzen, der mit dem Auftragsverarbeiter oder einem seiner verbundenen Unternehmen im Wettbewerb steht oder zur Durchführung der Prüfung nicht entsprechend qualifiziert ist. Der Verantwortliche wird seine Prüfungsrechte nicht öfter als einmal in einem Zwölf (12)-Monatszeitraum ausüben, außer (i) wenn und sofern dies wegen einer Weisung einer zuständigen Datenschutzaufsichtsbehörde oder einer anderen Regulierungsbehörde, die für den Verantwortlichen zuständig ist, erforderlich ist, oder (ii) wenn der Verantwortliche begründeterweise glaubt, dass eine weitere Prüfung aufgrund einer Verletzung oder vermuteten Verletzung der Sicherheit beim Auftragsverarbeiter notwendig ist.

(4) Der Auftragsverarbeiter ist bezüglich Folgendem nicht zur Offenlegung oder zur Gewährung von Zugriff verpflichtet: (i) Daten mit Bezug zu anderen Kunden (x) des Auftragsverarbeiters, (y) seiner verbundenen Unternehmen oder (z) eines Unterauftragsverarbeiters, (ii) interne Buchhaltungs- oder Finanzdaten oder Geschäftsgeheimnisse des Auftragsverarbeiters, seiner verbundenen Unternehmen oder eines Unterauftragsverarbeiters oder (iii) Informationen, die die Sicherheit von Systemen oder Geschäftseinrichtungen des Auftragsverarbeiters, seiner verbundenen Unternehmen oder eines Unterauftragsverarbeiters gefährden könnten.

10 Rückgabe oder Löschung Personenbezogener Daten bei Beendigung

Bei Beendigung dieser AVV wird der Auftragsverarbeiter, nach Wahl des Verantwortlichen, die im Rahmen der AVV verarbeiteten personenbezogenen Daten löschen oder diese Daten zurückgeben und vorhandene Kopien löschen, es sei denn, anwendbares Recht verlangt die Speicherung dieser Daten, solange diese Verpflichtung besteht.

11 Verschiedenes

Im Falle von Widersprüchen haben die Bestimmungen dieser AVV Vorrang vor den anderen Bestimmungen des Vertrages.

Appendix 1 zur AVV

Angaben zu personenbezogenen Daten und deren Verarbeitung:

Gegenstand der Verarbeitung personenbezogener Daten	Erbringung der Services gegenüber dem Verantwortlichen gemäß dem Vertrag (jeweils wie nachfolgend definiert). Die AVV ergänzt den Vertrag zwischen dem Auftragsverarbeiter und dem Verantwortlichen im Hinblick auf die Leistungen des Auftragsverarbeiters in Bezug auf den Betrieb der BuildingMinds Plattform und die Bereitstellung der BuildingMinds Plattform Services und/oder ergänzende Lieferungen oder Leistungen wie Professional Services (zusammen die „**Services**"), die die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen beinhalten oder beinhalten können (der „**Vertrag**"). Der Vertrag, auf dessen Grundlage die Services erbracht werden, kann (a) als Einzelvertrag auf der Grundlage eines Rahmenvertrags für Services (Master Service Agreement – „**MSA**"), (b) als Vertrag über einen Proof of Concept oder Onboarding-Leistungen oder (c) als individuell verhandelter Vertrag zwischen dem Auftragsverarbeiter und dem Verantwortlichen oder ihren jeweiligen verbundenen Unternehmen geschlossen werden. Soweit diese AVV keine eigenen Begriffsbestimmungen enthält, gelten die Begriffsbestimmungen des Vertrags und die Begriffe „**Auftragnehmer**" und „**Kunde**" beziehen sich auf die Parteien dieses Vertrags. Die jeweiligen Rollen des Auftragnehmers und der mit ihm verbundenen Unternehmen (gemeinsam „**BM-Gruppe**") in Bezug auf die Services sind nachfolgend spezifiziert. Alle Unternehmen der BM-Gruppe, die an der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen beteiligt sind, unterliegen konzerninternen Vereinbarungen, die sicherstellen, dass alle Unternehmen der BM-Gruppe zu jeder Zeit die Bedingungen dieser AVV einhalten. Für die Zwecke dieser AVV gilt das jeweilige Unternehmen der BM-Gruppe, das der Auftragnehmer im Rahmen des Vertrags ist, als Auftragsverarbeiter und alle anderen Unternehmen der BM-Gruppe, die an der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen beteiligt sind, gelten für Zwecke dieser AVV als Unterauftragsverarbeiter.
Art der Verarbeitung personenbezogener Daten	Verarbeitung personenbezogener Daten zur Erbringung der Services gemäß den Bestimmungen des Vertrags, einschließlich der in Art. 4 Nr. 2 DSGVO beschriebenen Vorgänge. Die jeweiligen Rollen und Verantwortlichkeiten der Unternehmen der BM-Gruppe in Bezug auf die Erbringung der Services sind im folgenden Abschnitt "Rollen und Zuständigkeiten / Unterauftragsverarbeiter" beschrieben.
Rollen und Zuständigkeiten / Unterauftragsverarbeiter	**Gruppeninterne Unterauftragsverarbeitungen** Die folgenden Unternehmen der BM-Gruppe werden wie im Abschnitt "Gegenstand der Verarbeitung personenbezogener Daten" angegeben entweder als Auftragsverarbeiter oder als Unterauftragsverarbeiter tätig: **BuildingMinds Technology AG** Rolle: Die BuildingMinds Technology AG, Seestrasse 55, 6052 Hergiswil (NW), Schweiz ist der zentrale Vertragspartner der BM-Gruppe für internationale Verträge und für internationale MSAs, die ihrerseits einen Rahmen für

	individuelle Verträge bilden können, und dient als zentraler Ansprechpartner für die Kunden. Die BuildingMinds Technology AG hat die Erbringung aller Services an die BuildingMinds GmbH vergeben. Die BuildingMinds GmbH hat die Kunden- und Vertragsverwaltung an die BuildingMinds Technology AG vergeben. Die BuildingMinds Technology AG hat daher, unabhängig davon, ob sie als Auftragnehmer auftritt oder nicht, Zugriff auf personenbezogene Daten ausschließlich zu Vertragsverwaltungs- und Abrechnungszwecken. Weitere Informationen zu Verarbeitungstätigkeiten und Unterauftragsverarbeitern finden Sie in der bei Abschluss der AVV gültigen Fassung des Dokuments „Wie wir personenbezogene Daten verarbeiten“ unter: https://buildingminds.com/de/prozessierung-personenbezogener-daten **BuildingMinds GmbH** Rolle: Die BuildingMinds GmbH, Schindler-Platz, 12105 Berlin, Deutschland ist die zentrale technische und operative Abwicklungseinheit der BM-Gruppe. Die BuildingMinds GmbH betreibt die BuildingMinds Plattform und erbringt alle Services, sei es als Auftragnehmer oder als Unterauftragnehmer anderer Unternehmen der BM-Gruppe. Die BuildingMinds GmbH hat daher Zugang zu allen personenbezogenen Daten, die im Auftrag des Verantwortlichen innerhalb der BM-Gruppe verarbeitet werden, und verarbeitet diese personenbezogenen Daten für die Erbringung der Services. Weitere Informationen zu Verarbeitungstätigkeiten und Unterauftragsverarbeitern finden Sie in der bei Abschluss der AVV gültigen Fassung des Dokuments „Wie wir personenbezogene Daten verarbeiten“ unter: https://buildingminds.com/de/prozessierung-personenbezogener-daten **Hosting der BuildingMinds Platform** Die BuildingMinds Plattform wird in der europäischen Azure-Cloud von Microsoft gehostet. Weitere Informationen zu Verarbeitungstätigkeiten und Unterauftragsverarbeitern finden Sie in der bei Abschluss der AVV gültigen Fassung des Dokuments „Wie wir personenbezogene Daten verarbeiten“ unter: https://buildingminds.com/de/prozessierung-personenbezogener-daten
Künftige Änderungen	Der Verantwortliche wird über jede beabsichtigte Hinzufügung oder Ersetzung von Unterauftragsverarbeitern, die gemäß diesem **Appendix 1** eingesetzt werden, gemäß Ziff. 8 der AVV informiert. Der Verantwortliche kann sich über künftige Änderungen der Verarbeitungstätigkeiten und Unterauftragsverarbeiter der einzelnen oben aufgeführten Unternehmen informieren, indem er regelmäßig die oben verlinkten Webseiten besucht. Der Verantwortliche hat die Möglichkeit, allen relevanten Änderungen gemäß den Bestimmungen der AVV zu widersprechen.
Arten der personenbezogenen Daten	Daten, die der Verantwortliche oder vom Verantwortlichen autorisierte Personen dem Auftragsverarbeiter durch Nutzung von Services gemäß dem Vertrag zur Verfügung stellen. Diese Daten können z. B. Folgendes umfassen: Name, Alter, Geburtsdatum und -ort sowie andere Identifizierungsmerkmale, die in Verträgen genutzt werden, Nutzungsgewohnheiten von Immobiliennutzern, private und dienstliche Kontaktinformationen (z.B. Telefon- und Faxnummern, E-Mail-Adresse, Postanschrift), Bankverbindungs- oder Rechnungsdaten, Datenbank- und

	Kalendereinträge, Nutzer-Name, Systemzugang, -einstellungen, -berechtigung, IP-Adresse, Zeitzone, Sprache und Unternehmensname.
Zweck der Verarbeitung personenbezogener Daten	Erbringung der Services gemäß den Bestimmungen des Vertrags
Kategorien betroffener Personen, auf die sich die personenbezogenen Daten beziehen	Personen, bezüglich derer der Verantwortliche oder vom Verantwortlichen autorisierte Personen dem Auftragsverarbeiter im Rahmen der Nutzung der Services Daten liefern. Diese Personen können z. B. sein: Der Verantwortliche, seine Lieferanten, Dienstleister oder andere Vertragspartner, die jeweiligen Mitarbeiter und andere Personen, wie z.B. Nutzer der Immobilien des Verantwortlichen.
Dauer der Verarbeitung personenbezogener Daten	Die Laufzeit des Vertrags zzgl. des Zeitraums zwischen Ende des Vertrags und Löschung der personenbezogenen Daten durch den Auftragsverarbeiter gemäß den Bestimmungen des Vertrags.

Appendix 2 zur AVV

Technische und organisatorische Maßnahmen

Die administrativen, physischen, organisatorischen und technischen Maßnahmen des Auftragsverarbeiters umfassen mindestens Folgendes:

I. Pseudonymisierung und Verschlüsselung

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um die Pseudonymisierung zu gewährleisten, falls erforderlich:

- *Gängige Pseudonymisierungsmaßnahmen dienen dazu, Namen und andere Identifikationsmerkmale mit Identifikatoren zu ersetzen. Ziel ist es, die Identifizierung der betroffenen Person zu verhindern oder erheblich zu erschweren.*
- *Die Pseudonymisierung wird mit Hilfe verschiedener Identifikatoren, wie z.B. Personal-, Mandanten- oder Kundencodes, durchgeführt. Es werden also keine echten Namen verwendet.*

Die personenbezogenen Daten des Verantwortlichen werden mit Hilfe von Verschlüsselungstechniken geschützt. Bei der Übertragung personenbezogener Daten innerhalb eines Netzwerks, d.h. zwischen Nutzergeräten und Rechenzentren oder innerhalb der Rechenzentren selbst, wird mindestens die TLS-Version 1.2 verwendet. Zum Schutz von gespeicherten personenbezogenen Daten (*data at rest*) werden eine Reihe von integrierten Verschlüsselungsfunktionen angeboten. Dabei werden die folgenden Verfahren eingesetzt:

- *Symmetrische Verschlüsselung: Mit Hilfe eines Schlüssels werden Informationen verschlüsselt und entschlüsselt.*
- *Asymmetrische Verschlüsselung: Mit Hilfe von zwei Schlüsseln, dem öffentlichen und dem privaten Schlüssel, werden Informationen ver- und entschlüsselt.*

II. Vertraulichkeit

Es werden strenge Maßnahmen ergriffen, um die personenbezogenen Daten des Verantwortlichen vor unrechtmäßigem Zugriff oder Verwendung durch Unbefugte zu schützen. Zu diesem Zweck wird der Zugang der Mitarbeiter eingeschränkt.

1. Zugangskontrolle von Personen

Der Auftragsverarbeiter ergreift die folgenden Schutzmaßnahmen, um zu verhindern, dass Unbefugte an die Datenverarbeitungsanlagen gelangen, in denen personenbezogene Daten verarbeitet oder genutzt werden:

- ***Physische Schutzmaßnahmen:***

  Der Zugang zu physischen Rechenzentrums-Einrichtungen ist durch externe und interne Zugangshindernisse geschützt. Die Sicherheitsrichtlinien weiten sich mit zunehmender Sicherheitsstufe aus. Dies wird durch den Einsatz von Sicherheitspersonal und durch verschlossene Serverschränke erreicht. Darüber hinaus werden Multifaktor-Zugangskontrollen durchgeführt. Eine integrierte Alarmanlage und eine 24/7-Videoüberwachung bieten weiteren Schutz vor Unbefugten.

- ***Systemseitige Schutzmaßnahmen:***

  Rollenbasierte Zugriffskontrolle, Multifaktor-Authentifizierung und die Minimierung des ständigen Zugriffs auf Produktionsdaten schränken das System gezielt ein. Der Zugriff auf die personenbezogenen Daten des Verantwortlichen wird vollständig protokolliert. Um sicherzustellen, dass dies ordnungsgemäß umgesetzt wird, werden regelmäßige Audits (sowie stichprobenartige Audits) durchgeführt.

2. Systemzugriffskontrolle

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um die Systeme zur Verarbeitung personenbezogener Daten vor der Nutzung durch Unbefugte zu schützen:

- *Personenbezogene Daten werden ausschließlich in sicheren Rechenzentren gespeichert (siehe Punkt 1 Zugangskontrolle von Personen).*
- *Der Systemzugang zu allen Systemen, die personenbezogene Daten verarbeiten, erfolgt über einen SSL-verschlüsselten Zugang.*
- *Personenbezogene Daten, die auf mobilen Datenträgern zwischengespeichert werden, sind verschlüsselt.*
- *Der Systemzugang zu Systemen, die personenbezogene Daten vereinbaren, erfordert eine besondere persönliche Berechtigung. Hierfür sind ein Passwort und ein zweiter Authentifizierungsfaktor erforderlich.*
- *Bei Mitarbeitern, die das Unternehmen verlassen, wird der Systemzugang innerhalb von 24 Stunden nach dem Ausscheiden entzogen.*

3. Datenzugriffskontrolle

Der Auftragsverarbeiter ergreift Maßnahmen, um sicherzustellen, dass die zur Nutzung eines Systems zur Verarbeitung personenbezogener Daten berechtigten Personen nur im Rahmen ihrer Zugriffsberechtigung auf personenbezogene Daten zugreifen können. Es werden Maßnahmen ergriffen, die verhindern, dass personenbezogene Daten während der Verarbeitung, der Nutzung und nach der Speicherung derselben unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Verantwortliche hat während der gesamten Vertragslaufzeit die Möglichkeit, seine in der BuildingMinds Plattform gespeicherten Daten einzusehen, auszulesen und zu löschen oder dies vom Auftragsverarbeiter zu verlangen.

- *Nur befugte Mitarbeiter dürfen entsprechend ihrer jeweiligen Rolle und Notwendigkeit Zugang zu personenbezogenen Daten erhalten. Auf diese Weise stellt der Auftragsverarbeiter sicher, dass die Mitarbeiter, die mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen befasst sind, diese nur auf Anweisung des Verantwortlichen verarbeiten. Darüber hinaus sind diese Personen verpflichtet, die Vertraulichkeit und Sicherheit der personenbezogenen Daten auch nach Beendigung ihrer Tätigkeit zu wahren.*
- *Alle autorisierten Personen benötigen eine besondere persönliche Autorisierung. Diese Authentifizierung erfordert ein Passwort und einen zweiten Authentifizierungsfaktor. Der authentifizierte Benutzer kann nur entsprechend der ihm zugewiesenen Rolle auf personenbezogene Daten zugreifen.*
- *Der Zugang von Mitarbeitern, die das Unternehmen verlassen haben, wird unmittelbar nach ihrem Ausscheiden gesperrt.*

- *Der Zugang kann nur von Administratoren gewährt werden. Die Anzahl der Administratoren ist auf das für den Betrieb der Systeme zur Verarbeitung personenbezogener Daten erforderliche Maß beschränkt.*
- *Die Einhaltung der Passwortrichtlinien wird durch die Systemtechnik sichergestellt und alle Anmeldungen werden im System protokolliert.*
- *Die Authentifizierungsmechanismen auf der Grundlage von Passwörtern müssen regelmäßig erneuert werden.*

4. Auftragskontrolle

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass personenbezogene Daten nur gemäß den Anweisungen des Verantwortlichen verarbeitet werden können:

- *Die personenbezogenen Daten werden nur für die im Vertrag festgelegten Zwecke verwendet.*
- *Im Verhältnis zwischen den Parteien behält sich der Verantwortliche alle Rechte und das Eigentum an seinen personenbezogenen Daten vor. Außer den vom Verantwortlichen gewährten Rechten erhält der Auftragsverarbeiter keine Rechte an den personenbezogenen Daten.*

5. Trennungskontrolle

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass die personenbezogenen Daten verschiedener Kunden getrennt verarbeitet werden können:

- *Die Daten einzelner Mandanten / Kunden werden explizit einem Kunden zugeordnet. Die Daten werden mit einer eindeutigen Kunden-ID gekennzeichnet und logisch getrennt im System gespeichert.*
- *Der Zugriff auf Daten erfordert immer eine Kunden-ID. Das System beschränkt den Zugriff auf diesen spezifischen Kunden.*

III. Integrität

1. Überwachung von Übermittlungen

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass personenbezogene Daten bei der elektronischen Übermittlung, beim Transport und bei der Speicherung auf Datenträgern nicht von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können:

- *Die erhobenen personenbezogenen Daten werden auf verschiedenen Ebenen geschützt.*
- *Zwischengespeicherte personenbezogene Daten werden verschlüsselt (siehe Punkt I Pseudonymisierung und Verschlüsselung).*
- *Die personenbezogenen Daten des Verantwortlichen werden nicht an staatliche Stellen weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben. Falls eine Strafverfolgungsbehörde die personenbezogenen Daten des Verantwortlichen anfordert, wird der Auftragsverarbeiter sie bitten, die Daten direkt bei dem Verantwortlichen anzufordern. Wird einem solchen Ersuchen stattgegeben, so wird der Verantwortliche unverzüglich informiert, sofern dies nicht gesetzlich verboten ist.*

- *Der Verantwortliche wird nach Erhalt eines Ersuchens um personenbezogene Daten des Verantwortlichen durch andere Dritte unverzüglich informiert, sofern dies nicht gesetzlich verboten ist.*

2. Eingabekontrolle

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass nachträglich kontrolliert und überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt wurden:

- *Benutzerkonten werden einzelnen Benutzern zugewiesen und können nicht auf mehrere verschiedene Benutzer aufgeteilt werden.*
- *Nur bestimmte Systemadministratoren haben Zugriff auf die im System gespeicherten Informationen, es sei denn, der Ersteller der Datei oder das Team, das das Dokument gemeinsam nutzt, hat Schreib- oder Lesezugriff gewährt.*
- *Das System protokolliert Einzelheiten darüber, wer zuletzt auf die personenbezogene Daten zugegriffen hat.*

IV. Verfügbarkeit und Resilienz

1. Verfügbarkeitskontrolle

Der Auftragsverarbeiter sorgt dafür, dass die technische Infrastruktur eine hohe Verfügbarkeit und Zuverlässigkeit bietet. In diesem Zusammenhang ergreift der Auftragsverarbeiter die folgenden Maßnahmen zum Schutz personenbezogener Daten vor zufälliger Zerstörung oder Verlust:

- *Unterbrechungsfreie Stromversorgungen verhindern bei kurzfristigen Stromausfällen einen ungeplanten Systemabsturz. Darüber hinaus werden Notstromaggregate eingesetzt, um die Stromversorgung bei längeren Stromausfällen zu übernehmen.*
- *Schnelle und robuste Glasfasernetze verbinden die Rechenzentren mit anderen großen Knotenpunkten und Internetnutzern.*
- *Darüber hinaus wird die Hochverfügbarkeit durch Überwachungsmaßnahmen und die daraus resultierende schnelle Reaktion auf Störungen sichergestellt.*
- *Geografisch verteilte Betriebszentren sind rund um die Uhr in Betrieb.*
- *Intelligente Back-up-Failover-Funktionen sorgen für die Verfügbarkeit.*
- *Die Daten werden permanent an zwei Standorten vorgehalten. Die Standorte der Backup-Sites können ausgewählt werden. Dadurch können einwandfreie Replikate erstellt werden.*

2. Wiederherstellbarkeit

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass die verwendeten Systeme im Falle eines Ausfalls wiederhergestellt werden können:

- *Es werden regelmäßig Wiederherstellungspunkte gespeichert, damit persönliche Daten wiederhergestellt werden können.*
- *Wenn ein Laufwerk einen Hardwarefehler aufweist, wird es sicher gelöscht oder zerstört, bevor es zum Austausch oder zur Reparatur an den Hersteller zurückgeschickt wird.*

V. Verfahren zur regelmäßigen Überprüfung, Beurteilung und Bewertung

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

Zur regelmäßigen Überprüfung der getroffenen technischen und organisatorischen Maßnahmen wird ein Datenschutzmanagement eingerichtet, damit diese gegebenenfalls angepasst werden können.