Ergänzende Bedingungen zur Verarbeitung von Daten im Auftrag

i.S.v. Art. 28 Abs. 3 EU-Datenschutzgrundverordnung („DSGVO“) (im Weiteren: „AV-Vereinbarung“) zwischen **Locaboo GmbH**, Balanstr. 73 / Haus 21A, 81541 München **(**nachfolgend: **Auftragnehmer** genannt**)** und dem Kunden (nachfolgend: **Auftraggeber** genannt) (gemeinsam nachfolgend: „**die Parteien**“)

1. Allgemeines

(1) Die AV-Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien, die sich aus der zwischen den Parteien vereinbarten Leistungserbringung des Auftragnehmers (gemäß den Allgemeinen Geschäftsbedingungen des Auftragnehmers und mitgeltender, die Leistungserbringung regelnder Dokumente) (im Weiteren: der „Hauptvertrag“) ergeben. Sie findet in diesem Zusammenhang Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO (im Weiteren: „Daten“) des Auftraggebers gemäß Art. 28 DSGVO verarbeiten. Sofern in dieser AV-Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(2) Der Auftragnehmer betreibt die SaaS-Applikation „Locaboo“ als Softwareplattform zur Termin- bzw. Raumplanung sowie zur Mitarbeiter- und Kundenverwaltung und stellt diese dem Auftraggeber zur Verfügung.

(3) Der Auftragnehmer verarbeitet ausschließlich personenbezogene Daten, die der Auftraggeber im Rahmen der Nutzung der vertraglich vereinbarten Leistungen bereitstellt oder durch die Nutzung der Leistungen erzeugt. Der Auftragnehmer stellt hierfür die technischen Möglichkeiten und die Software zur Verfügung.

2. Gegenstand, Art und Zweck der Verarbeitung

(1) Der Auftragnehmer führt im Auftrag des Auftraggebers für die Dauer der Vertragslaufzeit eine Verarbeitung personenbezogener Daten auf Grundlage des Hauptvertrages aus. Es gelten für die folgende AV-Vereinbarung die Begriffsbestimmungen (Legaldefinitionen) der DSGVO und des BDSG.

(2) Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag. Die Verarbeitung umfasst insbesondere die nachfolgend aufgeführten Verarbeitungsvorgänge, ohne dass hierdurch die Leistungspflichten aus dem Hauptvertrag erweitert oder neu bestimmt werden:

- Hosting der Datenbanken für die genannte SaaS-Applikation und des Webservers
- Entwicklung und Support der Software dieser Applikationen und der Schnittstellen zu weiterführenden IT-Systemen
- Tägliches Backup der Daten und Aufbewahrung gemäß den gesetzlichen Pflichten

(3) Bei dem Betrieb des Onlineportals werden regelmäßig folgende Arten von personenbezogenen Daten verarbeitet:

- Personenstamm- und Kontaktdaten der Nutzer (u.a. Name, E-Mail-Adresse, Telefonnummer)
- Daten zur Nutzung des Onlinedienstes (Zugangsdaten, IP-Adresse, sonstige Metadaten)
- Vertrags-, Abrechnungs- und Buchungsdaten

(4) Kategorien betroffener Personen:

- Mitarbeiter des Auftraggebers
- Endkunden des Auftraggebers

(5) Die personenbezogenen Daten werden für die Dauer des Hauptvertrages verarbeitet. Nach Beendigung des Hauptvertrages werden sie nach Maßgabe von Ziff. 10 gelöscht oder zurückgegeben, sofern nicht das Unionsrecht oder das Recht eines Mitgliedstaats eine weitere Speicherung verlangt.

3. Beginn, Dauer und Beendigung des Auftrags

(1) Diese AV-Vereinbarung tritt mit ihrem elektronischen Abschluss in Kraft und gilt für die Dauer des Hauptvertrages.

(2) Das Recht der Parteien zur außerordentlichen Kündigung bleibt unberührt. Der Auftraggeber ist ohne eine wirksame AV-Vereinbarung oder eine entsprechende Nachfolgevereinbarung nicht berechtigt, Leistungen des Auftragnehmers zu nutzen, die eine Auftragsverarbeitung personenbezogener Daten erfordern.

(3) Der Auftraggeber kann die AV-Vereinbarung aus wichtigem Grund ohne Einhaltung einer Frist kündigen, insbesondere wenn der Auftragnehmer schwerwiegend gegen anwendbare Datenschutzvorschriften oder gegen Pflichten aus dieser AV-Vereinbarung verstößt, eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder eine vertragsgemäße Kontrolle durch den Auftraggeber oder die zuständige Aufsichtsbehörde verweigert.

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und für die Rechtmäßigkeit der Verarbeitung sowie die Wahrung der Rechte betroffener Personen verantwortlich. Der Auftragnehmer unterstützt den Auftraggeber nach Maßgabe von Art. 28 Abs. 3 Satz 2 lit. e DSGVO bei der Bearbeitung von Anträgen betroffener Personen nach Kapitel III der DSGVO. Er stellt dem Auftraggeber die hierfür erforderlichen Informationen unverzüglich zur Verfügung und leitet Anfragen betroffener Personen, die erkennbar den Auftraggeber betreffen, unverzüglich an diesen weiter.

(2) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages und gemäß den Weisungen des Auftraggebers verarbeiten. Die Weisungen des Auftraggebers werden anfänglich durch diese AV-Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisungen). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst insbesondere Weisungen im Hinblick auf die Berichtigung und Löschung personenbezogener Daten sowie die Einschränkung ihrer Verarbeitung.

(3) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Vorliegen einer Rechtsgrundlage und die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO, verantwortlich. Der Auftragnehmer ist weder berechtigt noch verpflichtet, die Rechtmäßigkeit der vom Auftraggeber veranlassten Verarbeitung eigenständig zu prüfen, soweit keine Prüf- oder Hinweispflicht nach dieser AV-Vereinbarung oder dem anwendbaren Recht besteht.

(4) Änderungen des in Ziff. 2 festgelegten Gegenstands, der Art oder des Zwecks der Verarbeitung sowie wesentliche Verfahrensänderungen sind zwischen den Parteien abzustimmen und in Schrift- oder Textform zu dokumentieren.

(5) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser AV-Vereinbarung festgelegten Verpflichtungen zu überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei seiner Kontrolle feststellt.

(6) Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, außer in Notfällen) anzumelden und durch den Auftragnehmer zu unterstützen (z.B. durch Bereitstellung von Personal).

(7) Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragnehmers und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind.

(8) Der Auftragnehmer kann die Einhaltung seiner Verpflichtungen zunächst durch aktuelle Berichte unabhängiger Prüfer, genehmigte Verhaltensregeln nach Art. 40 DSGVO oder geeignete Zertifizierungen nach Art. 42 DSGVO nachweisen. Reichen diese Nachweise unter Berücksichtigung des konkreten Prüfungsanlasses nicht aus, bleibt der Auftraggeber berechtigt, eine angemessene Vor-Ort-Kontrolle nach Maßgabe der Absätze 5 bis 7 durchzuführen.

(9) Die Regelungen der Absätze 5 bis 8 gelten entsprechend für Kontrollen weiterer Auftragsverarbeiter. Solche Kontrollen erfolgen grundsätzlich unter Einbeziehung des Auftragnehmers, der seine vertraglichen Kontrollrechte gegenüber dem weiteren Auftragsverarbeiter ausübt.

5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer führt ausschließlich die Leistungen durch, die zur Erfüllung der beauftragten Leistungen erforderlich sind. Er führt sie ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Änderungen des Tätigkeitsfeldes und Verfahrensänderungen sind schriftlich zu vereinbaren. Der Auftragnehmer speichert oder verarbeitet personenbezogene Daten ausschließlich im Auftrag und auf Weisung des Auftraggebers. Der Auftragnehmer hat die zur Durchführung des Hauptvertrages notwendigen Leistungen so auszuführen, dass er sich nur insoweit Kenntnis von fremden Geheimnissen verschafft, als dies zur Vertragserfüllung erforderlich ist. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Für sämtliche Mitarbeiter des Auftragnehmers gilt aufgrund ihrer Aufgabenstellungen die Vertraulichkeit nach Art. 28 Abs. 3 lit. b DSGVO. Nach dieser Vorschrift ist es ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten. Gem. Art. 28 Abs. 3 lit. b DSGVO ist jeder Mitarbeiter verpflichtet, die Vertraulichkeit der verarbeiteten Daten zu wahren. Diese Verpflichtung besteht auch über das Ende seiner Tätigkeit im Unternehmen hinaus. Der Auftragnehmer verpflichtet sich in diesem Kontext, nur solche Mitarbeiter zur Durchführung der AV-Vereinbarung einzusetzen, die über Ihre Pflichten zur Vertraulichkeit und zur Einhaltung aller weiteren Datenschutzbestimmungen belehrt, auf die Rechtsfolgen von Verstößen (u.a. Strafbarkeit)

hingewiesen wurden und eine entsprechende Verpflichtungserklärung unterschrieben haben. Zudem setzt der Auftragnehmer davon unabhängig nur solche Mitarbeiter ein, bei denen keine Anhaltspunkte dafür ersichtlich sind, dass deren Verlässlichkeit eingeschränkt sein könnte. Darüber hinaus werden auch nur solche Mitarbeiter eingesetzt, die eine angemessene Ausbildung und/oder Berufserfahrung im Umgang mit personenbezogenen Daten Dritter und zur Durchführung der notwendigen Arbeiten des Hauptvertrages haben.
(3) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten zum Zwecke der Durchführung des Hauptvertrages.
(4) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im erforderlichen Umfang bei der Erfüllung der Rechte betroffener Personen sowie bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO. Dies umfasst insbesondere die Sicherheit der Verarbeitung, die Meldung von Verletzungen des Schutzes personenbezogener Daten, die Benachrichtigung betroffener Personen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Die hierfür erforderlichen Informationen stellt der Auftragnehmer dem Auftraggeber unverzüglich zur Verfügung.
(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
(6) Der Auftragnehmer berichtigt oder löscht personenbezogene Daten aus dem Auftragsverhältnis oder schränkt deren Verarbeitung ein, wenn der Auftraggeber dies anweist, sofern nicht das Unionsrecht oder das Recht eines Mitgliedstaats eine weitere Speicherung verlangt.
(7) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
(8) Über datenschutzrelevante Vorfälle und Verstöße gegen die vertraglichen Regelungen unterrichtet der Auftragnehmer den Auftraggeber unverzüglich.
(9) Die Parteien sind verpflichtet, alle ihnen im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und der anderen Vertragspartei vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser AV-Vereinbarung bestehen.

6. Datenschutzbeauftragter des Auftragnehmers
(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.
(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen, und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieser AV-Vereinbarung sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten. Änderungen hinsichtlich der Person oder der Kontaktdaten des Datenschutzbeauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich in Textform mit.

7. Meldepflichten des Auftragnehmers
(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.
(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht.

Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber gemäß Art. 33 Abs. 2 DSGVO insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung, einschließlich der Kategorien und der ungefähren Zahl betroffener Personen sowie der Kategorien und der ungefähren Zahl betroffener personenbezogener Datensätze;
- den Namen und die Kontaktdaten einer Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung; und
- eine Beschreibung der ergriffenen oder vorgeschlagenen Abhilfemaßnahmen einschließlich etwaiger Maßnahmen zur Abmilderung nachteiliger Auswirkungen.

Können die Informationen nicht gleichzeitig bereitgestellt werden, dürfen sie ohne unangemessene weitere Verzögerung schrittweise übermittelt werden.

8. Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine schriftliche Genehmigung, die in Anlage 2 aufgeführten weiteren Auftragsverarbeiter einzusetzen. Der Auftragnehmer informiert den Auftraggeber in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters. Der Auftraggeber kann innerhalb von zwei Wochen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund widersprechen. Können die Parteien keine einvernehmliche Lösung erzielen, kann die betroffene Leistung eingeschränkt oder beendet werden.
(2) Der Auftragnehmer wählt weitere Auftragsverarbeiter sorgfältig aus und verpflichtet sie durch Vertrag oder ein anderes Rechtsinstrument auf dieselben Datenschutzpflichten, die für ihn nach dieser AV-Vereinbarung gelten. Kommt ein weiterer Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.
(3) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf nur auf dokumentierte Weisung des Auftraggebers und unter Einhaltung der Art. 44 bis 49 DSGVO erfolgen. Der Auftragnehmer informiert den Auftraggeber über das jeweils eingesetzte Übermittlungsinstrument und stellt ihm auf Anfrage die erforderlichen Nachweise zur Verfügung.
(4) Nicht als Unterauftragsverhältnisse sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen und Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

9. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.
(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 1 zu dieser AV-Vereinbarung beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und

Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.
(3) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen.

10. Beendigung
(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrages oder jederzeit auf dessen Anforderung alle ihm etwaig überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer binnen vier Wochen nach erfolgter Löschungsanzeige zu kontrollieren. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

11. Zurückbehaltungsrecht
Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

12. Schlussbestimmungen
(1) Änderungen der AV-Vereinbarung: Änderungen und Ergänzungen dieser AV-Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(2) Gültigkeit der AV-Vereinbarung: Sollten einzelne Bestimmungen dieser AV-Vereinbarung unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien werden im Falle der Unwirksamkeit einer Klausel eine in sachlicher, am wirtschaftlichen Zweck des Vertrages orientierte, ersatzweise Regelung vereinbaren. Dies gilt sinngemäß für unvollständige Klauseln.
(3) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.
(4) Gerichtsstand, Anwendbares Recht: Auf diese AV-Vereinbarung gilt ausschließlich deutsches Recht einschließlich der Bestimmungen der DSGVO und unter Ausschluss des UN-Kaufrechts. Kollisionsrecht findet keine Anwendung. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser AV-Vereinbarung ist München, soweit eine solche Gerichtsstandsvereinbarung gesetzlich zulässig ist.
(5) Geschäftsbedingungen: Allgemeine Geschäfts- und Einkaufsbedingungen des Auftraggebers finden keine Anwendung auf diese AV-Vereinbarung. Diese AV-Vereinbarung gilt gegenüber dem Auftraggeber auch dann ausschließlich, wenn der Auftragnehmer seine Leistungen auch in Kenntnis entgegenstehender Allgemeiner Geschäfts- oder Einkaufsbedingungen vorbehaltslos ausführt.
(6) Rangfolge: Bei Widersprüchen zwischen Inhalten dieser AV-Vereinbarung und Bestimmungen des Hauptvertrags hinsichtlich datenschutzrechtlicher Themen gilt diese AV-Vereinbarung vorrangig. Im Übrigen bleiben die Bestimmungen des Hauptvertrages unberührt und gelten für diese AV-Vereinbarung entsprechend.

13. Elektronischer Abschluss und Schriftform
Der Abschluss dieser AV-Vereinbarung erfolgt in einem elektronischen Format und erfüllt damit das Schriftformerfordernis des Art. 28 Abs. 9 DSGVO.

Anlage 1 - Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Die Locaboo GmbH betreibt Ihre Server in zertifizierten Rechenzentren. Zertifikate und Beschreibungen der Sicherheitskonzepte können auf Anfrage gesondert bereitgestellt werden.

Es sind technisch-organisatorische Maßnahmen ergriffen worden, die ein angemessenes Datenschutzniveau und dessen Aufrechterhaltung gewährleisten:

a. Der Auftragsverarbeiter hat ein angemessenes Datenschutzmanagementsystem, bzw. ein Datenschutzkonzept implementiert und gewährleistet dessen Umsetzung.
b. Eine geeignete Organisationsstruktur für die Datensicherheit und Datenschutz ist vorhanden und die Informationssicherheit ist integriert in unternehmensweite Prozesse und Verfahren integriert
c. Es sind interne Sicherheitsricht- bzw. -leitlinien definiert, die unternehmensintern gegenüber Mitarbeitern als verbindliche Regeln kommuniziert werden.
d. Der Auftragsverarbeiter führt bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch. Das Verfahren ist entsprechend dem PDCA-Zyklus aufgebaut und besteht aus einer kontinuierlichen Beobachtung der technischen und organisatorischen Maßnahme sowie Festlegung des Istzustandes, als auch des zu erreichenden Soll-Zustandes mit folgender Umsetzungs- und sich daran anschließenden Überprüfungsphase sowie Evaluierung der Umsetzung und Ableitung der gewonnenen Erfahrungen für künftige Optimierungen und Vorgehen im Hinblick auf die Sicherheitsstandards.
e. Es werden regelmäßig und auch anlasslos System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests, durchgeführt.
f. Die technischen und organisatorischen Maßnahmen nach werden regelmäßig, mindestens jährlich, nach dem PDCA-Zyklus (Plan-Do-Check-Act) überprüft und angepasst.
g. Die Entwicklung des Standes der Technik und sowie der Entwicklungen, Bedrohungen und Sicherheitsmaßnahmen werden fortlaufend beobachtet und in geeigneter Art und Weise auf das eigene Sicherheitskonzept abgeleitet.
h. Es besteht ein Konzept, das die Wahrung der Betroffenenrechte durch den Auftraggeber gewährleistet (insbesondere im Hinblick auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche). Zu dem Konzept gehört die Unterrichtung der Mitarbeiter über die Informationspflichten gegenüber dem Auftraggeber, Einrichtung von Umsetzungsverfahren und die Benennung zuständiger Personen sowie regelmäßige Kontrolle und Evaluierung der ergriffenen Maßnahmen.
i. Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Gefährdungen und Verletzungen des Schutzes personenbezogener Daten gewährleistet. Zu dem Konzept gehört die Unterrichtung der Mitarbeiter über die Informationspflichten gegenüber dem Auftraggeber, Einrichtung von Umsetzungsverfahren und die Benennung zuständiger Personen sowie regelmäßige Kontrolle und Evaluierung der ergriffenen Maßnahmen.
j. Sicherheitsvorkommnisse werden konsequent dokumentiert, auch wenn sie nicht zu einer externen Meldung (z. B. an die Aufsichtsbehörde, betroffene Personen) führen (sogenanntes "Security Reporting").
k. Konsultation und Einbindung des Datenschutzbeauftragten bei Sicherheitsfragen und in Sicherheitsverfahren, die den Schutz personenbetroffener Daten betreffen.
l. Ausreichende fachliche Qualifikation des Datenschutzbeauftragten für sicherheits-relevante Fragestellungen und Möglichkeiten zur Fortbildung in diesem Fachbereich.

m. Ausreichende fachliche Qualifikation des IT-Sicherheitsbeauftragten für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung in diesem Fachbereich.
n. Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden (Wartungs-, Wach-, Transport- und Reinigungsdienste, freie Mitarbeiter, etc.), werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Sofern die Dienstleister im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten des Auftraggebers erhalten oder sonst das Risiko eines Zugriffs auf die personenbezogenen Daten besteht, werden sie speziell auf Verschwiegenheit und Vertraulichkeit verpflichtet.
o. Eingesetzte Software und Hardware wird stets auf dem aktuell verfügbaren Stand gehalten und Softwareaktualisierungen werden ohne Verzug innerhalb einer angesichts des Risikograde und eines eventuellen Prüfnotwendigkeit angemessenen Frist ausgeführt. Es wird keine Software und Hardware eingesetzt, die von den Anbietern im Hinblick auf Belange des Datenschutzes- und Datensicherheit nicht mehr aktualisiert wird (z. B. abgelaufene Betriebssysteme).
p. Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen.
q. Eine Geräteverwaltung erlaubt die Bestimmung, welche Beschäftigten oder Beauftragten welche Geräte in welchen Bereichen einsetzen.
r. Es wird ein „papierloses Büro“ geführt, d. h. Unterlagen werden grundsätzlich nur digital gespeichert und nur in Ausnahmefällen in Papierform aufbewahrt.
s. Unterlagen im Papierformat werden nur dann aufbewahrt, wenn keine im Hinblick auf die Auftragsverarbeitung, ihrem Zweck und den Interessen der von den Inhalten der Unterlagen betroffenen Personen adäquate digitale Kopie vorliegt oder eine Aufbewahrung mit dem Auftraggeber vereinbart wurde oder gesetzlich erforderlich ist.
t. Es liegt ein den Datenschutzanforderungen der Auftragsverarbeitung und dem Stand der Technik entsprechendes Lösch- und Entsorgungskonzept vor. Die physische Vernichtung von Dokumenten und Datenträgern erfolgt datenschutzgerecht und entsprechend den gesetzlichen Vorgaben, Branchenstandards und dem Stand der Technik entsprechenden Industrienormen. Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und soweit zuständig, über Vorgaben für die Datenvernichtung oder Gerätevernichtung durch Dienstleister unterrichtet.
u. Die Verarbeitung der Daten des Auftraggebers, die nicht entsprechend den Vereinbarungen dieses Auftragsverarbeitungsvertrages gelöscht wurden (z.B. in Folge der gesetzlichen Archivierungspflichten), wird im erforderlichen Umfang durch Sperrvermerke und/oder Aussonderung eingeschränkt.

Die nachfolgende Matrix beschreibt den Betrieb der SaaS-Plattformen, die sowohl die Anforderungen aus Art. 32 DSGVO als auch die Vorgaben des Cyber Resilience Act (CRA) berücksichtigen.

Kategorie	Maßnahmen (DSGVO + CRA)
1. Zutrittskontrolle	- Gesicherte Rechenzentren (ISO 27001) - Zugang nur für autorisierte Personen - Besucherprotokollierung
2. Zugangskontrolle	- MFA für alle Benutzer - Rollenbasierte Rechte - Passwort-Policy (kein Default) - CRA: Secure by Default

3. Zugriffskontrolle	- Least-Privilege-Prinzip - Logging aller Zugriffe - CRA: Zero-Trust-Architektur
4. Weitergabekontrolle	- TLS 1.3 für alle Datenübertragungen - VPN für interne Admin-Zugriffe - CRA: Verschlüsselung „in transit“
5. Eingabekontrolle	- Audit-Logs für Änderungen - Vier-Augen-Prinzip bei kritischen Prozessen
6. Auftragskontrolle	- AVV mit Subunternehmern - Prüfung auf DSGVO- und CRA-Konformität
7. Verfügbarkeitskontrolle	- Georedundante Backups - Disaster-Recovery-Tests - CRA: Nachweis Resilienz gegen Cyberangriffe
8. Trennungskontrolle	- Mandantenfähigkeit - Logische Datenisolierung - CRA: SBOM für eingesetzte Komponenten
9. Schwachstellenmanagement	- Regelmäßige Penetrationstests - Patch-Management - CRA: Koordinierte Schwachstellenmeldung (CVD)
10. Monitoring & Logging	- SIEM-System für Echtzeitüberwachung - CRA: Meldung von Sicherheitsvorfällen an zentrale Plattform
11. Datenschutzmaßnahmen	- Pseudonymisierung & Verschlüsselung personenbezogener Daten - Privacy by Design
12. Organisatorische Maßnahmen	- Schulungen zu DSGVO & Informationssicherheit - Sicherheitsbeauftragter im DevOps-Prozess - CRA: CE-Konformitätsdokumentation

Anlage 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Hinweis: Sämtliche nachfolgend aufgeführten Unternehmen gelten, soweit sie personenbezogene Daten zur Erbringung der jeweiligen Leistung im Auftrag verarbeiten, als Auftragsverarbeiter im Sinne von Art. 28 DSGVO. Die Beschreibung ihrer jeweiligen Funktion dient ausschließlich der näheren Erläuterung der von ihnen erbrachten Leistung.

Dabei handelt es sich um die nachfolgenden Unternehmen:

Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen, Deutschland	Rechenzentrumsleistungen und Hosting der für Locaboo verwendeten physischen Server und Webserver	Keine Drittlandübermittlung vorgesehen; Verarbeitung in Deutschland.
Loy GmbH	Königsdorfer-Str. 25 82515 Wolfratshausen, Deutschland	Programmierung	Keine Drittlandübermittlung vorgesehen; Verarbeitung in Deutschland.
Inxmail GmbH	Wentzingerstraße 17 79106 Freiburg, Deutschland	Locaboo-Mailversand	Keine Drittlandübermittlung vorgesehen; Verarbeitung in Deutschland.
Cloudflare, Inc.	101 Townsend Street San Francisco, California 94107 USA	Content Delivery Network (CDN), DNS-Dienste sowie Schutz vor DDoS-Angriffen und sonstigen Angriffen auf die Webanwendung	Angemessenheitsbeschluss der Europäischen Kommission zum EU-U.S. Data Privacy Framework~~;~~