Vereinbarung über die

Verarbeitung von Daten im Auftrag

(AV-Vereinbarung)

Zwischen den **Parteien des Leistungsvertrags** über die Nutzung der Software Planerio bestehend aus dem

Kunden als **„Auftraggeber“**

und der

Planerio GmbH, Theresienhöhe 11a, 80339 München, als **„Auftragnehmer“**

wird vereinbart:

1. Gegenstand und Merkmale der Datenverarbeitung im Auftrag

1.1. Diese AV-Vereinbarung regelt den Umgang mit personenbezogenen Daten durch den Auftragnehmer im Rahmen des zwischen den Parteien geschlossenen Leistungsvertrags (nachfolgend „**Leistungsvertrag**“). Die AV-Vereinbarung gilt hinsichtlich des Umgangs mit personenbezogenen Daten vorrangig vor dem Leistungsvertrag, bestehenden Geheimhaltungs- oder gesetzlichen Aufbewahrungspflichten des Auftragnehmers. Der Auftragnehmer verarbeitet die personenbezogenen Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 Datenschutz-Grundverordnung (DSGVO).

1.2. Gegenstand, Umfang, Art und Zweck der Datenverarbeitung ergeben sich aus dem Leistungsvertrag. Die Art der Verarbeitung (Art. 4 Nr. 2 DSGVO) der personenbezogenen Daten, die Kategorien der Betroffenen sowie weisungsberechtigte Personen und Weisungsempfänger sind in **Anlage 1** zu dieser AV-Vereinbarung geregelt. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

1.3. Die Laufzeit dieser AV-Vereinbarung entspricht der des Leistungsvertrags. Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt und dem Auftraggeber deshalb ein Festhalten am Vertrag nicht zugemutet werden kann.

1.4. Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Übermittlung oder

sonstige Verlagerung der Daten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. Rechte und Pflichten des Auftraggebers

2.1. Verantwortung für Datenverarbeitung

Der Auftraggeber bleibt ausschließlich berechtigt, über die Verarbeitung der Daten zu bestimmen. Der Auftraggeber trägt die Verantwortung für die Verarbeitung und ist gegenüber Dritten für die Einhaltung der Vorschriften der Datenschutzgesetze verantwortlich. Der Auftraggeber hat die datenschutzrechtliche Zulässigkeit der Auftragsdatenverarbeitung und des Auftrages eigenverantwortlich selbst zu beurteilen. Ist der Auftraggeber der Meinung, die Verarbeitung durch den Auftragnehmer verstoße gegen Pflichten des Auftraggebers, so hat er den Auftragnehmer hierauf hinzuweisen und eine rechtskonforme Datenverarbeitung durch entsprechende Weisungen sicherzustellen.

2.2. Mitteilungen, Unterstützung

Im Falle eines unmittelbaren Auskunftsverlangens, Hinweises, einer Warnung oder Anweisung der Aufsichtsbehörde gemäß Art. 58 DSGVO gegenüber dem Auftragnehmer, hat der Auftraggeber den Auftragnehmer zu unterstützen und sicherzustellen, dass dem behördlichen Verlangen im Einklang mit dieser AV-Vereinbarung Folge geleistet werden kann.

3. Pflichten des Auftragnehmers

3.1. Bindung an Weisungen

3.1.1. Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und gemäß den Weisungen des Auftraggebers. Dem Auftraggeber steht ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung zu, das er durch Einzelweisungen konkretisieren kann; unberührt davon bleiben gesetzliche Verpflichtungen des Auftragnehmers (z.B. bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a) DSGVO).

3.1.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in Textform über die vereinbarten Kommunikationskanäle. Mündlich erteilte Weisungen wird der Auftraggeber unverzüglich mindestens in Textform bestätigen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre von beiden Parteien aufzubewahren.

3.1.3. Verstößt eine Weisung oder eine beauftragte Datenverarbeitung gegen datenschutzrechtliche Vorschriften, so hat der Auftragnehmer den Auftraggeber umgehend darüber zu informieren (Art. 28 Abs. 3 Satz 3 DSGVO).

3.1.4. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und zu dokumentieren.

3.1.5. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, Daten unbefugt an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer vertragsgemäßen Datenverarbeitung erforderlich sind, sowie Speicherungen von Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

3.1.6. Der Auftragnehmer darf die personenbezogenen Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen.

3.1.7. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer erst nach Prüfung und Zustimmung durch den Auftraggeber erteilen, es sei denn der Auftragnehmer hat die Auskunft aufgrund gesetzlicher Pflicht oder rechtskräftiger behördlicher oder gerichtlicher Anordnung zu erteilen. Der Auftragnehmer ist verpflichtet, alle Anfragen bezüglich der von dieser AV-Vereinbarung geregelten Daten unverzüglich an den Auftraggeber weiterzuleiten, es sei denn der Auftragnehmer ist zur Herausgabe ohne Mitteilung an den Auftraggeber gesetzlich verpflichtet. Ziff. 3.6.4. bleibt unberührt.

3.2. Datengeheimnis und Verpflichtung zur Vertraulichkeit

3.2.1. Der Auftragnehmer stellt sicher, dass sämtliche seiner Mitarbeiter, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können oder sonst Kenntnis von Daten des Auftraggebers erlangen, vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet sind (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO).

3.2.2. Sonstige Dritte, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, sind entsprechend zur Vertraulichkeit zu verpflichten. Der Auftragnehmer stellt durch geeignete Maßnahmen sicher, dass Dritte, die Zugang zu den Daten des Auftraggebers haben, diese nicht über die zwischen den Vertragspartnern vereinbarten Verarbeitungsvorgänge hinaus verarbeiten und dass den Weisungen und Vorgaben des Auftraggebers nach diesem Vertrag auch durch die Dritten Folge geleistet wird.

3.3. Technische und organisatorische Maßnahmen

3.3.1. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

3.3.2. Der Auftragnehmer verpflichtet sich zur Umsetzung und Einhaltung der in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen (TOM) und gewährleistet, dass diese unter Berücksichtigung der Anforderungen des Art. 32 DSGVO festgelegt wurden und damit die Schutzziele wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt sind, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Der Auftragnehmer gewährleistet außerdem für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände offen, soweit keine vorrangigen schutzwürdigen Interessen, insbesondere Geheimhaltungsinteressen, des Auftragnehmers gegen die Offenlegung überwiegen.

3.3.3. Der Auftraggeber ist verpflichtet, dem Auftragnehmer vor Vertragsschluss und während dessen Laufzeit rechtzeitig alle erforderlichen Informationen bereitzustellen, die der Auftragnehmer für die Berücksichtigung der Anforderungen des Art. 32 DSGVO benötigt. Der Auftraggeber weist gesondert darauf hin, wenn besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet werden sollen oder sich aus anderen Gründen Besonderheiten ergeben, insbesondere eine erhöhte Eintrittswahrscheinlichkeit oder Schwere des Risikos für die Rechte und Freiheiten der Betroffenen besteht.

3.3.4. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat regelmäßig eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO).

3.3.5. Der Auftragnehmer kann gegenüber dem Auftraggeber die Umsetzung seiner technischen und organisatorischen Maßnahmen auch durch Vorlage aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. gemäß ISO/IEC 27001:2015) nachweisen.

3.3.6. Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer sind zu den üblichen Geschäftszeiten und ohne wesentliche Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchzuführen.

3.4. Einschaltung von Unterauftragnehmern

3.4.1. Die Beauftragung von Unterauftragnehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit gesonderter oder allgemeiner Zustimmung des Auftraggebers gestattet (Art. 28 Abs. 2 DSGVO).

3.4.2. Freigegebene Unterauftragnehmer sind in **Anlage 3** aufgeführt.

3.4.3. Im Übrigen erteilt der Auftraggeber mit Abschluss dieser Vereinbarung seine allgemeine Genehmigung zur Einschaltung von Unterauftragnehmern durch den Auftragnehmer. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Hinzuziehung, Änderung oder Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch durch den Auftraggeber erfolgt unverzüglich, spätestens innerhalb von einem Monat ab Kenntnis.

3.4.4. Der Auftragnehmer trägt Sorge dafür, dass er Unterauftragnehmer unter Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, anerkannte Standarddatenschutz-klauseln, genehmigte Verhaltensregeln).

3.4.5. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen dem Auftraggeber und dem Auftragnehmer auch gegenüber Unterauftragnehmern gelten. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Auftraggeber hat das Recht, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

3.4.6. Der Vertrag mit dem Unterauftragnehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). Die Weiterleitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

3.4.7. Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig und sorgfaltsgemäß zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer vertraglich auferlegt wurden.

3.4.8. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die für die Leistungserbringung erforderlich sind, zur allgemein anerkannten und üblichen Betriebsorganisation gehören und deren Einsatz für den Auftraggeber vorhersehbar sind (z. B. Telekommunikationsleistungen, Reinigungskräfte, etc.), auch wenn die Kenntnisnahme personenbezogener Daten im Einzelfall nicht ausgeschlossen werden kann. Der Auftragnehmer bleibt verpflichtet, angemessene und zumutbare Maßnahmen zur Gewährleistung des Schutzes und der Sicherheit der personenbezogenen Daten des Auftraggebers zu treffen.

3.5. Mitwirkung bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten

3.5.1. Die Wahrung der Betroffenenrechte gemäß Art. 12 - 22 DSGVO ist alleinige Verantwortung von Auftraggeber.

3.5.2. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer, z.B. zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber zur Entscheidung weiterleiten. Der Auftragnehmer hat nur nach ausdrücklicher Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Dies gilt nicht bei entsprechender gesetzlicher Verpflichtung und im Falle von Ziff. 3.7.4. Auskünfte an den Betroffenen oder an Dritte darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Für die Mitteilung vertraulicher Informationen des Auftraggebers an den Betroffenen gilt Ziffer 3.5.4.

3.5.3. Der Auftragnehmer ist im Rahmen der Erfüllung der Informationspflichten gemäß Art. 12 bis 14 DSGVO zur Mitwirkung verpflichtet, soweit die Informationen dem Auftraggeber nicht anderweitig vorliegen oder bereits übermittelt wurden.

3.5.4. Der Auftragnehmer ist lediglich verpflichtet, personenbezogene Daten an den Auftraggeber in dem Format herauszugeben, in dem er diese vom Auftraggeber zur Verarbeitung im Rahmen dieses Vertrages erhalten hat oder bestimmungsgemäß verarbeitet hat. Sowohl die Herausgabe in einem sonstigen strukturierten, gängigen und maschinenlesbaren Format als auch die Herausgabe direkt an den Betroffenen oder einen von diesem bestimmten weiteren Verantwortlichen sind nur auf der Grundlage einer ausdrücklichen Weisung geschuldet.

3.6. Unterstützung bei Datenpannen, Folgeabschätzungen, Beanstandungen

3.6.1. Der Auftragnehmer weist den Auftraggeber auf eine ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten nach dieser AV-Vereinbarung unverzüglich hin. Der Hinweis enthält eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze. Die Bewertung des mit der Verletzung verbundenen Risikos ist allein Sache des Auftraggebers. Der Auftragnehmer wirkt hieran durch Meldung der Verletzung sowie Bereitstellung von Informationen mit.

3.6.2. Der Auftragnehmer ist zur Mitwirkung im Rahmen einer Datenschutz-Folgeabschätzung verpflichtet, soweit der Auftraggeber für die vorzunehmende Bewertung des Risikos der Verarbeitung neben den vom Auftragnehmer nach dieser Vereinbarung zur Verfügung zu stellenden Informationen noch weitere Auskünfte benötigt.

3.6.3. Sollen Empfehlungen der Aufsichtsbehörde gemäß Art. 36 Abs. 2 DSGVO Grundlage der Verarbeitung nach dieser AV-Vereinbarung werden, so hat der Auftraggeber diese durch ausdrückliche Weisung zu bestätigen. Dies gilt insbesondere auch für Empfehlungen, welche die Aufsichtsbehörde direkt dem Auftragnehmer gibt. Der Auftragnehmer informiert den Auftraggeber über ihm mitgeteilte Empfehlungen und Fristverlängerungen der Aufsichtsbehörde gemäß Art. 36 Abs. 2 DSGVO.

3.6.4. Der Auftragnehmer informiert den Auftraggeber über sonstige Beanstandungen, Anfragen oder Ersuchen hinsichtlich der Datenverarbeitung seitens Aufsichtsbehörden oder Betroffener, insbesondere über Kontrollhandlungen, Ermittlungen oder sonstige Maßnahmen von Aufsichtsbehörden, sofern geltendes Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.6.5. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Auskünfte erteilen. Dies betrifft insbesondere auch Informationen zur Abwehr von Ansprüchen Dritter oder im Hinblick auf Anforderungen von Aufsichtsbehörden.

3.7. Herausgabe und Löschung von Daten

3.7.1. Der Auftragnehmer setzt Löschanweisungen des Auftraggebers gemäß den nachfolgenden Absätzen um. Die Löschung in Live-Systemen erfolgt unmittelbar, die Löschung in Back-Up-Systemen spätestens nach 30 Tagen.

3.7.2. Der Auftraggeber ist berechtigt, jederzeit während der Laufzeit dieses Vertrages die Herausgabe oder Löschung der gespeicherten Daten zu verlangen. Ein Zurückbehaltungsrecht des Auftragnehmers ist insofern ausgeschlossen.

3.7.3. Nach Ende des Leistungsvertrages löscht der Auftragnehmer die Daten des Auftraggebers oder gibt sie auf dessen Wunsch heraus.

3.7.4. Erteilt der Auftraggeber dem Auftragnehmer eine verbindliche Löschungsanweisung schriftlich oder in einem dokumentierten elektronischen Format, so ist der Auftragnehmer verpflichtet, die Datenlöschung unverzüglich durchzuführen. Hiervon ausgenommen sind lediglich die Daten, hinsichtlich derer der Auftragnehmer gesetzlich zur Aufbewahrung verpflichtet ist. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

3.7.5. Dokumentationen, die dem Nachweis der auftrags- und vertragsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren oder können dem Auftraggeber übergeben werden.

3.8. Informations- und Kontrollmitwirkungspflichten

3.8.1. Der Auftraggeber darf die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen einschließlich der technischen und organisatorischen Maßnahmen gemäß Anlage 2 selbst oder durch Dritte kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen, Stichproben und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragnehmer ist verpflichtet, bei diesen Kontrollen unterstützend mitzuwirken.

3.8.2. Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer den Auftraggeber auf Anfrage die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutz- oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erbracht werden.

3.8.3. Im Rahmen dieser Ziff. 3.8. ist der Auftragnehmer lediglich zur Duldung und Mitwirkung bei einer jährlichen Vor-Ort-Kontrolle verpflichtet. Zur Duldung und Mitwirkung an darüber hinausgehenden Kontrollen, insbesondere durch Mehrfachprüfungen, ist der Auftragnehmer nur gegen Erstattung der ihr hierdurch entstehenden zusätzlichen Kosten verpflichtet. Dies gilt nicht für Kontrollen, die aufgrund eines Sicherheitsvorfalles bzw. eines mehr als unwesentlichen Verstoßes gegen die Pflichten gemäß dieser AV-Vereinbarung erforderlich werden.

3.9. Datenschutzbeauftragter

Der Auftragnehmer hat gemäß den gesetzlichen Vorgaben den/die Datenschutzbeauftragte(n) gemäß Anlage 1 bestellt. Soweit in Anlage 1 kein Datenschutzbeauftragter genannt ist, versichert der Auftragnehmer, dass keine gesetzliche Notwendigkeit für eine Bestellung vorliegt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

4. Haftung

4.1. Der Auftragnehmer haftet dem Auftraggeber nur für schuldhaft verursachte Pflichtverletzungen nach Maßgabe der entsprechenden Regelungen des Leistungsvertrages.

4.2. Soweit eine Haftung des Auftragnehmers beschränkt oder ausgeschlossen ist, stellt der Auftraggeber den Auftragnehmer von allen Ansprüchen frei, die Dritte wegen der Datenverarbeitung im Auftrag gegen den Auftragnehmer erheben.

5. Allgemeine Bestimmungen

5.1. Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

5.2. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

5.3. Der Auftragsverarbeiter ist berechtigt, diese AV-Vereinbarung anzupassen, sofern dies a) zur Erfüllung gesetzlicher oder regulatorischer Anforderungen, b) für technische oder sicherheitsrelevante Verbesserungen oder c) zur Optimierung der Vertragsdurchführung erforderlich ist. Der Auftragsverarbeiter informiert den Auftraggeber über wesentliche Änderungen mit einer Frist von mindestens 30 Tagen in Textform (z. B. per E-Mail). Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang der Mitteilung schriftlich Widerspruch erheben. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Änderung als genehmigt.

5.4. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

5.5. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, so bleibt die Gültigkeit im Übrigen unberührt.

5.6. Das Rechtsverhältnis zwischen den Vertragspartnern unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland. Die Bestimmungen des Wiener UN-Übereinkommens über Verträge über den internationalen Warenkauf vom 11. April 1980 finden keine Anwendung. Ausgeschlossen sind auch diejenigen Bestimmungen des deutschen Rechts, die zur Anwendung ausländischen Rechts führen.

5.7. Für alle Streitigkeiten im Zusammenhang mit dieser AV-Vereinbarung wird der Sitz des Auftragnehmers als ausschließlicher Gerichtsstand vereinbart. Der Auftragnehmer bleibt berechtigt, den Auftraggeber an dessen allgemeinen Gerichtsstand zu verklagen.

Anlage 1: Einzelheiten zur Datenverarbeitung, Ansprechpartner, Datenschutzbeauftragter des Auftragnehmers

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

Anlage 3: Freigegebene Unterauftragnehmer

Anlage 1
zur Vereinbarung über die Verarbeitung von Daten im Auftrag (AV-Vereinbarung)

Einzelheiten zur Datenverarbeitung, Ansprechpartner, Datenschutzbeauftragter des Auftragnehmers

---

1.) Art der Verarbeitung (Art. 4 Nr. 2 DSGVO):

- Erheben
- Erfassen
- Organisation
- Ordnen
- Speicherung
- Anpassung oder Veränderung
- Auslesen
- Abfragen
- Verwendung
- Offenlegung durch Übermittlung
- Verbreitung oder eine andere Form der Bereitstellung
- Abgleich oder die Verknüpfung
- die Einschränkung, das Löschen oder die Vernichtung

2.) Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

- Nachname, Vorname, Titel
- Adressdaten
- Personalkennnummern
- Arbeitsvertragsdaten (z.B. Arbeitstage, Arbeitszeiten, Urlaubstage, Gehälter, Lohn, Überstundenregelungen)
- Sonstige Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Qualifikationen und Qualifikationsziele
- Zeitstempel- (z.B. Einloggen, Ausloggen, Dienstgang) und Arbeitszeitdaten
- An- und Abwesenheitszeiten und -gründe
- Urlaubs-, Fortbildungs- und Dienstwünsche und -anträge

- Mitarbeiterpräferenzen (z.B. für Schichten, Arbeitszeiten, Einsatzorte, Arbeitsplätze, Teammitglieder)
- Sonstige Dienstplanungsdaten
- Lohn- und Gehaltsdaten
- In die ePersonalakte hochgeladene Dateien
- Vertragsstammdaten (Vertragsbeziehung, Vertragsinteresse)
- Historie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Nutzungsdaten

3.) Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

- Kunden
- Interessenten
- Aktuelle und ehemalige Mitarbeiter
- Bewerber
- Unterauftragnehmer
- Geschäftspartner
- Administratoren
- Ansprechpartner

4.) Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

- Alle Geschäftsführer und Prokuristen des Auftraggebers.

Weisungsempfänger beim Auftragnehmer sind:

- Cagatay Karakaya, +49 (0) 89 693 1998 0, c.karakaya@planerio.de
- Dr. Stefan Klußmann, +49 (0) 89 693 1998 0, s.klussmann@planerio.de

Einzelheiten zur Datenverarbeitung, Ansprechpartner, Datenschutzbeauftragter des Auftragnehmers

---

Für Weisung zu nutzende Kommunikationskanäle sind:

- Per Post: Planerio GmbH, Theresienhöhe 11A, 80339 München
- Per Email: datenschutz@planerio.de
- Per Telefon: +49 (0) 89 693 1998 0

5.) Datenschutzbeauftragter des Auftragnehmers:

Datenschutzbeauftragter der Planerio GmbH

c/o TÜV SÜD Akademie GmbH

Westendstraße 160

80339 München

E-Mail: datenschutz@planerio.de

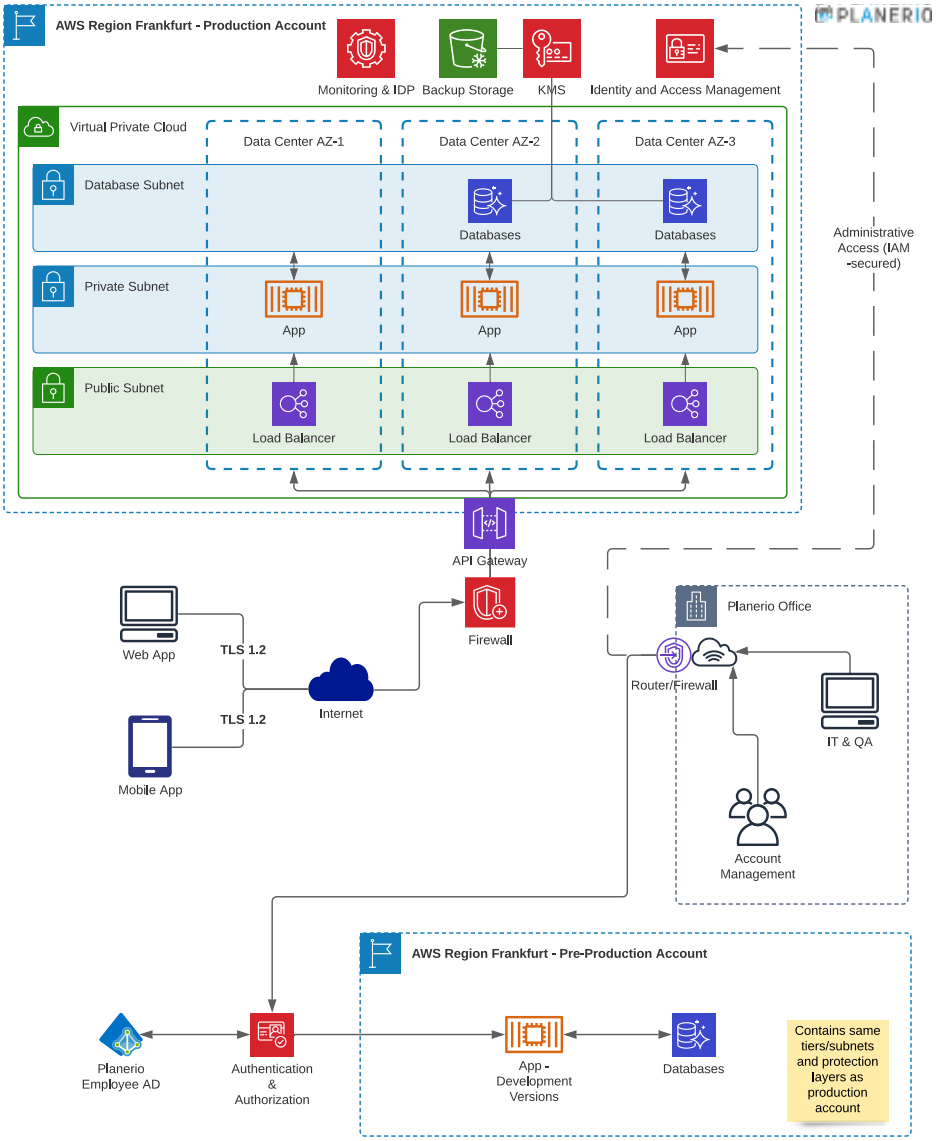
Anlage 2
zur Vereinbarung über die Verarbeitung von Daten im Auftrag (AV-Vereinbarung)

Technische und organisatorische Maßnahmen

---

1. Einleitung

Die folgende Darstellung bietet eine Übersicht über die benutzten Dienste und Systeme. Alle Verbindungen, die über das Internet hergestellt werden, sind bezüglich Integrität und Verfügbarkeit durch die jeweiligen Internetdienstleister geschützt.
In den folgenden Kapiteln werden die einzelnen Untersysteme hinsichtlich der Sicherheits- und Schutzmaßnahmen – gemäß Art. 32 DSGVO – beschrieben.



Übersicht über Dienste und Systeme

2. Planerio Büro

Grundregeln zum Datenschutz	Umsetzung durch Planerio GmbH
Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	
Allgemein:	- Verpflichtende Schulung und Überprüfung der Mitarbeitenden zu Datenschutz und IT-Sicherheit
Zutrittskontrolle:	- Sicherung von Planerio Büro und des gesamten Gebäudes mit unabhängigen Schließanlagen
Zugangskontrolle:	- Laptops mit Zugriff auf Cloud-Anwendungen und das Rechenzentrum unseres Cloud Service Providers mit Passwörtern gesichert (Minimalanzahl an Zeichen und Mindestanforderungen an die Synthax) - Verpflichtende 2-Faktor-Authentifizierung
Zugriffskontrolle:	- Minimalprinzip bei Zugriffsberechtigung der Mitarbeitenden von Planerio. Nur Entwicklung mit Zugriff auf Quellcode. Nur Geschäfts- und IT-Leitung mit Zugriff auf IT-Infrastruktur. Support & Sales mit Zugriff auf Cloud-Anwendungen zur Kunden-Kommunikation und Analyse des Nutzerverhaltens.
Trennungskontrolle:	- Trennung der Daten in der Datenbank durch logische Trennung (Mandantentrennung) - Schulung aller Nutzer in der Verwendung der Datenbanken - Trennung von Test- und Produktivsystemen - Einrichtung von Zugriffsrechten zu Anwendungen nur bei Erfordernis
Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
Weitergabekontrolle:	- WLAN verschlüsselt (WPA2, Schlüssellänge 32, Qualität 192 Bit) - Router mit Firewall - Laptops mit Personal Firewall - Verbindungen zwischen Cloud-Anwendungen (Server) und Client TLS-gesichert - Verbindungen zu Datenbanken durch SSH-Tunnel mit (Public/Private-Key) gesichert
Eingabekontrolle:	- Nicht relevant in Bezug auf Planerio Büro. Siehe Eingabekontrolle unter Rechenzentrum.
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)	
Verfügbarkeitskontrolle:	- Regelmäßige Durchführung von Backups (Backup-und Wiederherstellungsstrategie) - Firewall

Verfahrung zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)	
Auftragskontrolle:	- Verarbeitung von Daten nach Weisung des Auftraggebers durch einen Nutzungsvertrag - Keine Datenverarbeitung ohne vorherige Weisung des Auftraggebers - Abschluss von Vereinbarungen über die Verarbeitung von Daten im Auftrag (AV-Vereinbarung) im Falle von Auftragsdatenverarbeitung sowohl als Autragnehmer als auch als Auftraggeber
Datenschutz- und Incident-Response-Management:	- Datenschutzkonzept und Schweregrad-abhängige Verfahrensanweisungen im Falle eines Datenschutz-Incidents (Incident-Response-Management) - Regelmäßiger Review und ggf. Anpassung aller Datenschutz- und IT-Sicherheits-relevanten Komponente.

3. Rechenzentrum

Grundregeln zum Datenschutz	**Umsetzung durch Betreiber des Rechenzentrums**
Allgemein	
Ort der Datenspeicherung und -verarbeitung:	- Vertragliche Limitierung der Datenspeicherung und -verarbeitung auf die AWS-Region Frankfurt (aktuell bestehend aus drei physikalischen Rechenzentren im Großraum Frankfurt am Main) - Vertragliche Beschränkung aller genutzten Dienste explizit auf den EU-/EWR-Raum
Zertifizierungen und Nachweis der IT-Sicherheit:	- Nur Einsatz von Services, die gemäß des Cloud Computing Compliance Catalogue (C5) Standards geprüft sind - Zertifizierungen gemäß ISO 27001, 27017, 27018 sowie ISO 9001 - Nachweis der Effektivität der ISO 27018 durch Prüfung gemäß der Systems and Organizational Controls (SOC) halbjährlich im SOC 2-Bericht zum Datenschutz - FIPS 140-2 Zertifizierung des Key Management Systems (KMS) - Unter Aufsicht des BSI als Betreiber Kritischer Infrastruktur und Reporting gemäß entsprechend des Branchenspezifischen Standards (B3S)

Anlage 2
zur Vereinbarung über die Verarbeitung von Daten im Auftrag (AV-Vereinbarung)

Technische und organisatorische Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	
Zutrittskontrolle:	- Festlegung von Sicherheitsbereichen - Festlegung zutrittsberechtigter Personen - Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus - Protokollierung des Zutritts - Realisierung eines wirksamen Zutrittsschutzes - Begleitung von Besuchern und Fremdpersonal - Überwachung der Räume außerhalb der Betriebszeiten
Zugangskontrolle:	- Festlegung befugter Personen - Umsetzung sicherer Zugangsverfahren und Zugangsschutz (Authentisierung) - Protokollierung des Zugangs - Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk - Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen - Automatische oder manuelle Zugangssperre
Zugriffskontrolle:	- Berechtigungskonzepte mit Vergabe minimaler Berechtigungen - Umsetzung von Zugriffsbeschränkungen - Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
Trennungskontrolle:	- Vorhandensein von Richtlinien, Arbeitsanweisungen und Verfahrensdokumentation - Regelungen zur System- und Programmprüfung - Umsetzung eines Abstimm- und Kontrollsystems

Anlage 2
zur Vereinbarung über die Verarbeitung von Daten im Auftrag (AV-Vereinbarung)

Technische und organisatorische Maßnahmen

Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
Allgemein:	- Technische Maßnahmen zur Integritätssicherung (z.B. Hash-Berechnung, Replikationslogiken) - Regelmäßige automatische Integritätsprüfungen
Weitergabekontrolle:	- Festlegung empfangs-/weitergabe-berechtigter Instanzen/Personen - Sichere Datenübertragung zwischen Server und Client - Risikominimierung durch Netzseparierung mit Implementation von Sicherheitsgateways an den Netzübergabepunkten - Sichere Ablage von Daten, inkl. Backups - Prozess zur Sammlung und Entsorgung - Nutzung datenschutzgerechter Lösch- und Zerstörungsverfahren mit Führung von Löschprotokollen
Eingabekontrolle:	- Protokollierung der Eingaben - Dokumentation der Eingabeberechtigungen
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)	
Allgemein:	- Anwendungsarchitektur mit 2- bis 3-facher Redundanz in der AWS Region Frankfurt - Elastic Load Balancing - Auto-Scaling - Schutzmechanismen vor Distributed Denail of Service (DDoS) Attacken - Vorhandensein und Umsetzung eines Konzeptes zur Durchführung von regelmäßigen Datensicherungen - Vorhandensein und regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen - Überwachung der Betriebsparameter der Rechenzentren - Vorhandensein eines Notfallkonzeptes - Regelungen zur Aufnahme eines Krisen bzw. Notfallmanagements - Vertraglich zugesicherte SLAs

Verfahrung zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)	
Auftragskontrolle:	- Abschluss einer Vereinbarung über die Verarbeitung von Daten im Auftrag (AV-Vereinbarung) bzw. eines Data Processing Addendum (DPA) gemäß Anforderungen der DSGVO mit Nutzung von Standard Contractual Clauses - Protokollierung der Auftragsausführung durch den Auftragnehmer
Datenschutz- und Incident-Response-Management:	- Aktuelles, DSGVO-konformes Datenschutzkonzept - Definiertes Incident-Response-Management-System

4. WebApplikation planer.io

Grundregeln zum Datenschutz	**Umsetzung durch Planerio GmbH**
Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	
Allgemein:	- Nutzung von Zugriffskontrollen des Identity und Access Management (IAM) Services, um auf technischer Ebene Zugriffe auf z.B. gespeicherte Daten zu steuern
Zutrittskontrolle:	- Siehe 3. Rechenzentrum
Zugangskontrolle:	- Benutzerauthentisierung gemäß OWASP Empfehlung
Zugriffskontrolle:	- Benutzerauthentisierung gemäß OWASP Empfehlung - Festlegung individueller Rechte (Lesen, Schreiben) durch Administrator auf Standort- und Accountebene - Rechtevergabe Planerio-intern nach dem „Need-to-Know“-Prinzip
Trennungskontrolle:	- Mandantentrennung, d.h. verschiedene Kunden oder Auftraggeber können bedient werden, ohne dass diese gegenseitigen Einblick in ihre Daten, Benutzerverwaltung o.ä. bekommen - Getrennte Test- und Produktivsysteme ohne Vermischung von Produktiv- und Testdaten

Verschlüsselung:	- Verschlüsselung über AWS Key Management System (KMS). - „At rest“ Verschlüsselung von allen von Planerio eingesetzten Datenbanken - „In transit“ Transportverschlüsselung, wenn Daten über ein unsicheres oder öffentliches Netzwerk übertragen werden - Webinterface und API der Planerio-App ausschließlich über HTTPS-Verbindungen erreichbar mit Clients mit mindestens TLS 1.2 - Kein Zugriff von Mitarbeitenden des Cloud Service Providers auf Kunden-Schlüssel oder -Daten
Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
Weitergabekontrolle:	- Übertragung aller Daten TLS-verschlüsselt
Eingabekontrolle:	- Verwendung von AWS Cloudtrail - Protokollierung des Eingehens aller HTTP(S)-Requests mit Hilfe von Log-Entries
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)	
Verfügbarkeitskontrolle:	- Siehe 3. Rechenzentrum - Einsatz verschiedener Monitoring-Tools zur Überwachung der Verfügbarkeit und Performance
Verfahrung zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)	
Auftragskontrolle:	- Keine Verarbeitung personenbezogener Daten ohne Beauftragung - Datenverarbeitung innerhalb von planer.io gemäß Vorgaben des Auftraggebers
Datenschutz- und Incident-Response-Management:	- Datenschutzkonzept und Schweregrad-abhängige Verfahrensanweisungen im Falle eines Datenschutz-Incidents (Incident-Response-Management) - Falls verbunden mit Cloud Service Provider, siehe auch 3. Rechenzentrum

5. SmartPhone-Applikation Planerio

Grundregeln zum Datenschutz	**Umsetzung durch Planerio GmbH**
Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	
Zutrittskontrolle:	- Siehe 3. Rechenzentrum
Zugangs- und Zutrittskontrolle:	- Zugangskontrolle zum SmartPhone in der Verantwortung des Nutzers - Zugang zur Planerio-App durch Passwort geschützt

Technische und organisatorische Maßnahmen

Trennungskontrolle:	- Mandantentrennung, d.h. verschiedene Kunden oder Auftraggeber können bedient werden, ohne dass diese gegenseitigen Einblick in ihre Daten, Benutzerverwaltung o.ä. bekommen - Getrennte Test- und Produktivsysteme ohne Vermischung von Produktiv- und Testdaten
Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
Weitergabekontrolle:	- Optionaler PIN-, Muster-, Fingerabdruck-Schutz des SmartPhones (wie vom Nutzer eingestellt) - Wenn mit Planerio synchronisiert, dann Datenübertragung TLS-verschlüsselt
Eingabekontrolle:	- Protokollierung des Eingehens aller HTTP(S)-Requests mit Hilfe von Log-Entries
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)	
Verfügbarkeitskontrolle:	- Verfügbarkeit ist an Verfügbarkeit des SmartPhones bzw. Anbindung an das Internet gekoppelt - Falls verbunden mit Cloud Service Provider, siehe auch 3. Rechenzentrum
Verfahrung zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)	
Auftragskontrolle:	- Mit Installation der SmartPhone-App und Akzeptieren der Nutzungsbedingungen erfolgt Auftragserteilung an Planerio zur Datenverarbeitung gemäß des vom Kunden gebuchten Funktionsumfangs
Datenschutz- und Incident-Response-Management:	- Datenschutzkonzept und Schweregrad-abhängige Verfahrensanweisungen im Falle eines Datenschutz-Incidents (Incident-Response-Management) - Falls verbunden mit Cloud Service Provider, siehe auch 3. Rechenzentrum

Anlage 3
zur Vereinbarung über die Verarbeitung von Daten im Auftrag (AV-Vereinbarung)

Freigegebene Unterauftragnehmer

Name	Anschrift	Auftragsinhalt
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855 Luxembourg	- Hosting von Servern (Planerio-Applikation)
Kombo Technologies GmbH	Kottbusser Damm 25-26 10967 Berlin	- Automatisierung von Datenübergaben/ Schnittstellen
Mailjet GmbH	Rankestr. 21 10789 Berlin	- Automatisiertes Versenden von Emails
Microsoft Ireland Operations, Ltd.	One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	- Email-Kommunikation und Datenspeicherung (Office 365)
Monday.com Ltd.	6 Yitzhak Sadeh Street Tel Aviv 6777506 Israel	- Projektmanagement-Software Monday
n8n GmbH	Borsigstr. 27 10115 Berlin	- Automatisierung von Datenübergaben/ Schnittstellen
OneSignal, Inc.	411 Borel Ave, Ste 512 San Mateo, CA 94402 USA	- Push-Nachrichten für Smartphone App
Pendo.io, Inc.	150 Fayetteville St #1400 Raleigh, NC 27601 USA	- User Onboarding Software Pendo
Zendesk, Inc.	1019 Market Street San Francisco, CA 94103 USA	- Kundensupport