Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 EU-Datenschutz-Grundverordnung (DS-GVO)

(Elektronischer Abschluss, welcher als rechtsverbindlich gilt)

Zwischen

-Auftraggeber-

und

COPROG e.K.
Gastland 3
26826 Weener
Deutschland
-Auftragnehmer-

Diese Vereinbarung regelt die Auftragsverarbeitung personenbezogener Daten gemäß Art. 28 Abs. 3 der Datenschutz-Grundverordnung (DS-GVO) zwischen den Parteien. Etwaige zuvor zwischen den Parteien geschlossene Vereinbarungen zur Auftragsdatenverarbeitung auf Grundlage des § 11 BDSG a.F. werden hiermit beendet und durch diese Vereinbarung ersetzt.

Vorwort:

Diese Vereinbarung beschreibt die datenschutzrechtlichen Pflichten der Vertragsparteien, die aus dem Hauptvertrag zur Leistungserbringung entstehen. Sie legt fest, unter welchen Bedingungen der Auftragnehmer personenbezogene Daten für den Auftraggeber verarbeitet. Die Vereinbarung gilt für alle Tätigkeiten und Dienstleistungen, bei denen der Auftragnehmer im Rahmen des Hauptvertrags personenbezogene Daten des Auftraggebers verarbeitet.

Sie umfasst alle Datenverarbeitungen, die der Auftragnehmer im Zusammenhang mit den vertraglich vereinbarten Leistungen durchführt. Diese Vereinbarung sorgt dafür, dass alle gesetzlichen Anforderungen der Datenschutz-Grundverordnung (DS-GVO) und anderer relevanter Datenschutzgesetze eingehalten werden.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Der Gegenstand und die Dauer der Auftragsverarbeitung richten sich nach dem Hauptvertrag zur Leistungserbringung. Diese Vereinbarung gilt für die gesamte Laufzeit des Hauptvertrags, soweit personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden.

1.1. Gegenstand der Auftragsverarbeitung:

Die Verarbeitung personenbezogener Daten erfolgt durch den Auftragnehmer im Auftrag des Auftraggebers zum Zweck der Nutzung des COPROG Kalenders, einschließlich der Online-

Terminbuchung.

1.2. Betroffene Personen und Datenkategorien:

Betroffene Personen sind insbesondere:

a. Mitarbeiter des Auftraggebers
b. Kunden des Auftraggebers
c. Interessenten des Auftraggebers

Die Verarbeitung umfasst folgende Datenkategorien:

a. Vertragsstammdaten (z.B. Abrechnungs- und Zahlungsdaten, Bankverbindung, Firmenname)
b. Kommunikationsdaten (z.B. Telefon, E-Mail, Mobiltelefon)
c. Kundenhistorie (z.B. Interaktionen und Transaktionen)
d. Nutzungsdaten (z.B. Daten zur Nutzung der Dienstleistung und der Produkte: Log-Daten, Geräteinformation)
e. Zeitstempel (z.B. Terminvereinbarung, Terminverschiebung, Stornierung, Zahlung)
f. Zahlungsdaten (z.B. PayPal-Transaktionsdaten, Bankdaten)
g. IP-Adresse

1.3. Zusatzinformation:

Zusätzlich zu den oben genannten Daten kann die Auftragsverarbeitung folgende Tätigkeiten umfassen:

a. **Erfassung und Verarbeitung von Fotos:** Die Applikationen des Auftragnehmers ermöglichen es den Benutzern, Fotos aufzunehmen, die im Rahmen der Verarbeitung personenbezogener Daten verwendet werden können.
b. **Hochladen von Dokumenten:** Die Applikationen bieten die Funktionalität, Dokumente hochzuladen, die ebenfalls personenbezogene Daten enthalten können (z.B. Anamnesebogen, Hautanalyse). Diese Funktionalitäten sind in den nativen und Web-Applikationen des Auftragnehmers integriert und dienen ausschließlich der vereinbarten Auftragsverarbeitung.

Der Auftraggeber ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten sowie für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer verantwortlich. Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen der Weisungen des Auftraggebers und gemäß den in dieser Vereinbarung festgelegten Bedingungen.

1.4. Art und Zweck der Datenverarbeitung

Im Rahmen der Erbringung der vertraglich vereinbarten Leistungen erfolgt die Verarbeitung personenbezogener Daten gemäß der DS-GVO. Die Art der Verarbeitung umfasst insbesondere die Erhebung, Speicherung, Nutzung, Übermittlung und Löschung personenbezogener Daten.
Die Zwecke der Verarbeitung sind wie folgt:

a. Erfüllung der vertraglichen Leistungen: Die Verarbeitung dient der Erfüllung der im Hauptvertrag und in der Leistungsbeschreibung definierten vertraglichen Leistungen, einschließlich der Erfassung und Speicherung von Fotos und Dokumenten.
b. Bereitstellung von IT-Infrastruktur: Speicherung und Sicherung der Daten im Rahmen der Cloud-Hosting-Dienste des Auftragnehmers oder eines vom Auftragnehmer beauftragten Subunternehmers. Der Subunternehmer ALL-INKL.COM – Neue Medien Münnich ist für die Bereitstellung der Cloud-Infrastruktur zuständig. Die Einzelheiten zur Datenverarbeitung

durch ALL-INKL.COM entnehmen Sie der Datenschutzerklärung unter folgendem Link: https://all-inkl.com/datenschutzinformationen

c. Verwaltung und Unterstützung: Die Datenverarbeitung kann der Verwaltung und Unterstützung der Nutzung der Applikationen dienen, einschließlich der Verwaltung von Benutzerkonten und der Bearbeitung von Anfragen.

d. Diagnose und Wartung: Fernzugriffe zur Diagnose und Wartung, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann.

e. Erfüllung gesetzlicher Verpflichtungen: Die Verarbeitung kann erforderlich sein, um gesetzliche Verpflichtungen zu erfüllen, z.B. hinsichtlich Buchhaltungs- und Archivierungspflichten.

f. Zahlungsabwicklung: Die Verarbeitung personenbezogener Daten erfolgt über den Zahlungsdienstleister PayPal zur Abwicklung von Online-Transaktionen der Kunden des Auftraggebers. Dabei werden Zahlungsinformationen (z.B. Zahlungs-Betrag) an PayPal übermittelt. PayPal agiert als eigenständiger Verantwortlicher und der Auftragnehmer hat keinen Einfluss auf die datenschutzrechtlichen Maßnahmen des Zahlungsdienstleisters. Der Auftraggeber informiert die betroffenen Personen über die Datenverarbeitung durch PayPal und verweist auf die entsprechende Datenschutzerklärung. Er ist verpflichtet, die Kunden angemessen über diese Verarbeitung zu informieren, beispielsweise in seiner eigenen Datenschutzerklärung.

g. Verwaltung der Nutzerkonten: Verwaltung und Pflege von Nutzerkonten

h. Authentifizierung und Autorisierung: Sicherstellung des Zugriffs auf die Dienste durch Authentifizierung und Autorisierung.

i. Optimierung der App-Funktionen: Verbesserung der Funktionen und Benutzerfreundlichkeit der Applikation.

j. Weitere Verarbeitungszwecke: Dazu gehören Marketing, Fehleranalyse und optional spezifische Dienstleistungen, wie Analyse von Nutzerverhalten und Push-Benachrichtigungen. Die Einholung der Einwilligung der betroffenen Personen kann hierfür erforderlich sein.

1.5. Kategorien betroffener Personen:

Kategorien betroffener Personen sind insbesondere:

a. Kunden und Interessenten des Auftraggebers:
Personen, die Produkte oder Dienstleistungen des Auftraggebers erwerben oder in Anspruch nehmen. Dies kann Einzelpersonen oder Vertreter von Unternehmen umfassen.

b. Beschäftigte des Auftraggebers (z.B. Ansprechpartner)
Personen, die im Rahmen von Arbeits- oder Beschäftigungsverhältnissen beim Auftraggeber tätig sind, einschließlich derjenigen, die Zugang zu den von den Applikationen verarbeiteten Daten haben.

c. Kontaktpersonen und Vertreter: Personen, die als Ansprechpartner oder Vertreter für den Auftraggeber fungieren, beispielsweise in geschäftlichen Beziehungen oder bei der Kommunikation mit dem Auftragnehmer.

d. Benutzer der Applikationen: Personen, die die vom Auftragnehmer bereitgestellten nativen und Web-Applikationen nutzen. Dies kann sowohl interne Benutzer des Auftraggebers als auch externe Nutzer umfassen.

1.6. Die Dauer der Auftragsverarbeitung:

Die Dauer der Auftragsverarbeitung ist an die Laufzeit des Hauptvertrags gebunden. Die Verarbeitung der personenbezogenen Daten endet mit der Beendigung des Hauptvertrags, es

sei denn, eine längere Aufbewahrungsfrist ist gesetzlich vorgeschrieben oder erforderlich. Der Auftraggeber ist für die Einhaltung der gesetzlichen Aufbewahrungsfristen verantwortlich.

1.7. Arten der Applikationen

Der Auftragnehmer bietet sowohl native Applikationen (Software, die direkt auf den Geräten der Benutzer installiert wird) als auch Web-Applikationen (über das Internet zugängliche Software) an. Diese Applikationen werden zur Verarbeitung der oben genannten personenbezogenen Daten verwendet.

a. **Native Applikationen**: Die Software, die lokal auf den Endgeräten der Benutzer installiert wird und zur Verarbeitung der personenbezogenen Daten dient.
b. **Web-Applikationen**: Die Software, die über das Internet zugänglich ist und zur Verarbeitung der personenbezogenen Daten dient.

Die genaue Spezifikation der Applikationen und ihrer Funktionen wird in der Leistungsbeschreibung des Hauptvertrags detailliert beschrieben.

§ 2 Einsatz von Subunternehmern

2.1. Der Auftragnehmer ist berechtigt, Subunternehmer für die Erbringung der vertraglichen Leistungen einzusetzen, sofern der Auftraggeber dem Einsatz dieser Subunternehmer zugestimmt hat. Eine aktuelle Liste der eingesetzten Subunternehmer wird dem Auftraggeber auf Anfrage zugänglich gemacht.

2.3 Der Auftragnehmer stellt sicher, dass mit jedem eingesetzten Subunternehmer ein Auftragsverarbeitungsvertrag gemäß Artikel 28 DSGVO abgeschlossen wird. Dieser Vertrag verpflichtet den Subunternehmer, die gleichen datenschutzrechtlichen Pflichten zu erfüllen wie der Auftragnehmer im Hauptvertrag mit dem Auftraggeber. Insbesondere stellt der Auftragnehmer sicher, dass die Subunternehmer geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten ergreifen und die Verarbeitung nur auf Weisung des Auftragnehmers erfolgt.

2.4 Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Austausch von Subunternehmern schriftlich oder elektronisch. Der Auftraggeber hat das Recht, innerhalb von 14 Tagen nach Erhalt dieser Information Einwände gegen die Hinzuziehung oder den Austausch von Subunternehmern zu erheben.

2.5 Der Einsatz von Subunternehmern außerhalb des Europäischen Wirtschaftsraums (EWR) bedarf einer zusätzlichen Vereinbarung und Einhaltung der Vorgaben gemäß Kapitel V der DSGVO (z.B. durch Abschluss von Standardvertragsklauseln).

§ 3 Anwendungsbereich und Verantwortlichkeit

3.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag zur Leistungserbringung und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

3.2. Die Weisungen werden anfänglich durch den Hauptvertrag zur Leistungserbringung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer benannte Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag zur Leistungserbringung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 4 Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen des Auftrags und gemäß den Weisungen des Auftraggebers, es sei denn, es liegt ein Ausnahmefall nach Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, dass eine Weisung gegen anwendbares Recht verstößt, und setzt die Umsetzung der Weisung aus, bis eine Bestätigung oder Änderung durch den Auftraggeber erfolgt.

4.2. Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes entspricht, und trifft technische sowie organisatorische Maßnahmen zum angemessenen Schutz der Daten gemäß Art. 32 DS-GVO. Diese Maßnahmen gewährleisten die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung. Der Auftraggeber ist über diese Maßnahmen informiert und trägt die Verantwortung für deren Angemessenheit in Bezug auf die Risiken der verarbeiteten Daten. Änderungen der Sicherheitsmaßnahmen sind dem Auftragnehmer vorbehalten, dürfen jedoch das vertraglich vereinbarte Schutzniveau nicht unterschreiten.

4.3. Der Auftragnehmer unterstützt den Auftraggeber, soweit vereinbart, bei der Erfüllung von Anfragen betroffener Personen gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der Pflichten aus den Artikeln 33 bis 36 DS-GVO.

4.4. Der Auftragnehmer stellt sicher, dass alle Mitarbeiter und Personen, die mit der Datenverarbeitung betraut sind, die Daten nur im Rahmen der Weisungen verarbeiten und sich zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Pflicht bleibt auch nach Beendigung des Auftrags bestehen.

4.5. Der Auftragnehmer informiert den Auftraggeber unverzüglich über bekannt gewordene Verletzungen des Schutzes personenbezogener Daten und trifft erforderliche Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen. Die Abstimmung mit dem Auftraggeber erfolgt umgehend.

4.6. Der Auftragnehmer benennt dem Auftraggeber einen Ansprechpartner für datenschutzrelevante Fragen im Rahmen des Hauptvertrags.

4.7. Der Auftragnehmer gewährleistet die Einhaltung von Art. 32 Abs. 1 lit. d) DS-GVO und setzt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ein.

4.8. Der Auftragnehmer berichtigt oder löscht die verarbeiteten Daten auf Anweisung des Auftraggebers. In besonderen Fällen erfolgt die Aufbewahrung oder

Übergabe nach gesonderter Vereinbarung.

4.9. Nach Beendigung des Auftrags sind Daten auf Verlangen des Auftraggebers herauszugeben. Kosten bei der Herausgabe trägt der Auftraggeber. Die Kosten werden individuell, je nach Aufwand ermittelt und dem Auftraggeber mitgeteilt. 30 Tage nach Beendigung des Vertragsverhältnisses wird der Auftragnehmer alle auf dem Server gespeicherten Daten des Auftraggebers unwiderruflich löschen.

4.10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person gemäß Art. 82 DS-GVO verpflichtet sich der Auftragnehmer, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Abwehr des Anspruchs zu unterstützen.

§ 5 Pflichten des Auftraggebers

5.1. Der Auftraggeber verpflichtet sich, den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Ergebnissen der Auftragsverarbeitung Fehler oder Unregelmäßigkeiten hinsichtlich datenschutzrechtlicher Bestimmungen feststellt. Die Meldung hat innerhalb von 48 Stunden nach Entdeckung der Unregelmäßigkeit zu erfolgen.

5.2. Der Auftraggeber stellt sicher, dass alle personenbezogenen Daten, die an den Auftragnehmer übermittelt werden, den Anforderungen der DSGVO entsprechen. Dazu gehört die Implementierung geeigneter technischer und organisatorischer Maßnahmen, um die Sicherheit der Datenverarbeitung zu gewährleisten.

5.3. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 10 entsprechend. Der Auftraggeber hat den Auftragnehmer in diesem Fall unverzüglich zu informieren und ihn bei der Abwehr solcher Ansprüche angemessen zu unterstützen.

5.4. Der Auftraggeber benennt dem Auftragnehmer einen Ansprechpartner für datenschutzrechtliche Fragen, die im Rahmen des Hauptvertrages zur Leistungserbringung entstehen. Der Auftraggeber verpflichtet sich, den Auftragnehmer umgehend über Änderungen der Kontaktdaten zu informieren. Der Ansprechpartner hat die Aufgabe, Informationen bereitzustellen und die Kommunikation zwischen den Parteien zu erleichtern.

5.5. Der Auftraggeber verpflichtet sich zur aktiven Kooperation mit dem Auftragnehmer sowie mit Aufsichtsbehörden, um die Einhaltung der Datenschutzvorschriften zu überprüfen. Dies umfasst die Bereitstellung von Informationen und Zugang zu relevanten Unterlagen. Informationen bereitzustellen und die Kommunikation zwischen den Parteien zu erleichtern.

5.6. Der Auftraggeber sorgt dafür, dass seine Mitarbeiter, die mit der Verarbeitung personenbezogener Daten befasst sind, regelmäßig über Datenschutzbestimmungen geschult und für datenschutzrechtliche Themen sensibilisiert werden.

5.7. Der Auftraggeber stellt sicher, dass die an den Auftragnehmer übermittelten, personenbezogenen Daten klar definiert sind hinsichtlich des Umfangs, der Art und des Zwecks der Datenverarbeitung.

§ 6 Anfragen betroffener Personen

6.1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist.

6.2. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich nach Eingang an den Auftraggeber weiter, unabhängig davon, ob die Zuordnung zum Auftraggeber sofort möglich ist oder nicht.

6.3. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner technischen und organisatorischen Möglichkeiten auf Weisung des Auftraggebers, soweit dies vertraglich vereinbart ist oder gesetzlich vorgeschrieben wird.

6.4. Der Auftragnehmer haftet nicht für Verzögerungen, Fehler oder Unterlassungen des Auftraggebers bei der Beantwortung von Ersuchen betroffener Personen, sofern der Auftragnehmer seine in diesem Vertrag geregelten Pflichten ordnungsgemäß erfüllt hat. Der Auftragnehmer haftet jedoch für die Nichterfüllung seiner eigenen Pflichten gemäß diesem Vertrag und der DSGVO.

§ 7 Nachweismöglichkeiten

7.1. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf geeignete Weise den Nachweis über die Einhaltung der in dieser Vereinbarung festgelegten Pflichten zu erbringen. Der Auftragnehmer kann hierfür unter anderem folgende Informationen zur Verfügung stellen:
a. Ergebnisse eines Selbstaudits,
b. interne Verhaltensregeln

7.2. Sollte eine Inspektion durch den Auftraggeber oder einen von ihm beauftragten Prüfer erforderlich sein, wird diese nach Möglichkeit online durchgeführt. Der Auftragnehmer bittet um eine Vorlaufzeit von mindestens 30 Tagen zur Planung, um einen reibungslosen Ablauf zu gewährleisten. Der Auftragnehmer behält sich vor, die Durchführung der Inspektion von einer vorherigen Anmeldung sowie der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen, um die Vertraulichkeit der Daten anderer Kunden und der implementierten technischen und organisatorischen Maßnahmen zu schützen. Bei einem Wettbewerbsverhältnis mit dem Prüfer hat der Auftragnehmer das Recht, Einspruch zu erheben. Der Auftragnehmer berechnet für Bereitstellung der Unterstützungsleistungen bei Inspektionen eine Vergütung in Höhe von 120EUR /Stunde.

7.3. Sollte eine Datenschutzaufsichtsbehörde oder eine andere hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. In diesem Fall ist keine Unterzeichnung einer Verschwiegenheitsverpflichtung erforderlich, wenn die Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei deren

Verstoß strafrechtliche Konsequenzen drohen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

8.1. Sollte es zu Pfändungen, Beschlagnahmen, Insolvenzverfahren, Vergleichsverfahren oder sonstigen Maßnahmen Dritter kommen, die die Daten des Auftraggebers beim Auftragnehmer gefährden, wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren. Der Auftragnehmer wird alle in diesem Zusammenhang handelnden Personen, insbesondere Behörden oder Vollstreckungsorgane, unverzüglich darüber informieren, dass die Verfügungsgewalt und die Datenhoheit über die betroffenen Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

8.2. Änderungen und Ergänzungen dieser Vereinbarung und ihrer Bestandteile — einschließlich etwaiger Zusicherungen des Auftragnehmers — bedürfen einer schriftlichen Vereinbarung, die auch in Textform (z.B. per E-Mail) erfolgen kann, und müssen ausdrücklich als Änderung oder Ergänzung dieser Vereinbarung gekennzeichnet sein. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

8.3. Im Falle von Widersprüchen zwischen den Regelungen dieser Vereinbarung zum Datenschutz und den Regelungen des Hauptvertrages zur Leistungserbringung haben die datenschutzrechtlichen Regelungen dieser Vereinbarung Vorrang. Sollte eine Bestimmung dieser Vereinbarung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

8.4. Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

9.1 Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, soweit ausdrücklich etwas anderes vereinbart wurde.

9.2 Der Auftragnehmer haftet gemäß den gesetzlichen Bestimmungen für Schäden aus der Verletzung von Leben, Körper oder Gesundheit. Für andere Schäden haftet der Anbieter nur bei Vorsatz oder grober Fahrlässigkeit. Bei Schäden, die auf der Verletzung wesentlicher Vertragspflichten beruhen, haftet der Anbieter auch bei einfacher Fahrlässigkeit, jedoch nur für vorhersehbare Schäden zum Zeitpunkt der Vertragsverletzung. Diese Regelungen gelten auch für Pflichtverletzungen durch Erfüllungsgehilfen des Anbieters. Die Haftung nach dem Produkthaftungsgesetz sowie für Garantien bleibt hiervon unberührt.

9.3 Im Übrigen haftet der Anbieter nur, soweit er eine wesentliche Vertragspflicht (Kardinalpflicht) verletzt hat. In diesen Fällen ist die Haftung auf den Ersatz des vorhersehbaren, typischerweise eintretenden Schadens begrenzt.

9.4 Für einen einzelnen Schadenfall ist die Haftung auf den Vertragswert begrenzt, bei laufender Vergütung auf die Höhe der Vergütung pro Vertragsjahr, max. jedoch 250.000,00 EUR für Vermögensschäden und max. 3.000.000,00 EUR pauschal für Personen- und Sachschäden.

9.5 Der Anbieter haftet nicht für den Verlust von Daten, wenn der Kunde es versäumt hat, regelmäßig und in angemessenen Abständen Datensicherungen durchzuführen, sofern ihm die technische Möglichkeit dazu zur Verfügung stand.

Eine Haftung des Anbieters ist ausgeschlossen, wenn die Wiederherstellung der Daten nur mit unverhältnismäßigem Aufwand möglich ist. Der Anbieter haftet nur dann, wenn der Datenverlust auf eine grob fahrlässige oder vorsätzliche Pflichtverletzung des Anbieters zurückzuführen ist.

Hinweis: Diese Vereinbarung erfolgt mittels elektronischer Zustimmung.

Auftragnehmer	**Auftraggeber**
Ort:	Ort:
Datum:	Datum:
Inhaber/ Geschäftsführer:	Inhaber/ Geschäftsführer:
Unterschrift:	Unterschrift:

Anhang: Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DS-GVO

Technische und organisatorische Maßnahmen (TOMs)

1. Technische Maßnahmen

1.1 Zugriffskontrollen

- **Starke Authentifizierung: Nutzung von starken, komplexen Passwörtern für alle Benutzerkonten.**
- **Benutzerrechte: Regelmäßige Überprüfung und Anpassung der Zugriffsrechte basierend auf den Rollen der Benutzer.**

1.2 Datenverschlüsselung

- **Transportverschlüsselung: Verwendung von HTTPS für alle Datenübertragungen, um die Vertraulichkeit der Daten zu gewährleisten.**
- **Datenverschlüsselung im Ruhezustand: Sensible Daten werden vor der Speicherung in der Cloud verschlüsselt.**

1.3 Sicherheitsprotokolle

- **Firewalls: Einsatz von Firewalls, um unbefugten Zugriff zu verhindern.**

- **Regelmäßige Updates: Implementierung von automatischen Sicherheitsupdates für alle verwendeten Softwarelösungen.**

1.4 Backup und Recovery

- **Regelmäßige Datensicherung: Tägliche Backups aller relevanten Daten, die in der Cloud gespeichert sind, und Speicherung an einem sicheren Ort.**
- **Wiederherstellungsplan: Dokumentation eines klaren Plans zur Wiederherstellung von Daten im Falle eines Verlusts.**

1.5 Monitoring und Logging

- **Überwachung: Einsatz von Monitoring-Tools zur kontinuierlichen Überwachung von Zugriffen auf Daten und Systemaktivitäten.**
- **Protokollierung: Aufzeichnung aller relevanten Aktionen, um die Nachverfolgbarkeit zu gewährleisten.**

---

2. Organisatorische Maßnahmen

2.1 Vertragliche Regelungen

- **Auftragsverarbeitungsvertrag: Abschluss eines AVV mit allen Cloud-Anbietern, um die Einhaltung der DSGVO sicherzustellen.**

2.2 Schulung der Mitarbeiter

- **Regelmäßige Schulungen: Durchführung von Schulungen für alle Mitarbeiter zu Themen wie Datenschutz, Datensicherheit und Erkennung von Phishing-Versuchen.**

2.3 Richtlinien und Verfahren

- **Datenschutzrichtlinien: Erstellung und Implementierung interner Datenschutzrichtlinien, die regelmäßig überprüft und aktualisiert werden.**

2.4 Notfallmanagement

- **Notfallplan: Entwicklung und Dokumentation eines Notfallplans für den Fall von Datenpannen oder Sicherheitsvorfällen.**
- **Regelmäßige Tests: Durchführung von regelmäßigen Übungen zur Überprüfung der Notfallmaßnahmen.**

2.5 Dokumentation und Nachweis

- **Protokollführung: Dokumentation aller Sicherheitsmaßnahmen, Zugriffsrechte und Schulungsmaßnahmen. Nachweis der Einhaltung: Bereitstellung von Nachweisen über die Umsetzung der TOMs zur Transparenz gegenüber Aufsichtsbehörden und betroffenen Personen.**