Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DS-GVO

zwischen

Kunden des Dienstes Terminpilot.de

– Verantwortlicher - nachfolgend „**Auftraggeber**“ genannt –

und

Terminpilot.de, betrieben durch die Papke Media GmbH & Co KG, Johann-Krane-Weg 8, 48149 Münster

– Auftragsverarbeiter - nachfolgend „**Auftragnehmer**“ genannt –

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den zwischen den Parteien in ihren Einzelheiten beschriebenen vertraglichen Auftragsverarbeitungen ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

Die Vereinbarung kommt durch Akzeptanz des Kunden im Rahmen der Log-In zustande und wird automatisch Vertragsbestandteil.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien / Kreis betroffener Personen
Namen, Adressen, Kontaktdaten	Vereinbarung von Terminen, Ansprache von Kunden	Kunden, Endkunden

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten **im Auftrag** des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages 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).
(2) Die **Weisungen** werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor.
(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstoßt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

§ 4 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Bestimmungen dieses Vertrags und den Weisungen des Auftraggebers erhebt und verwendet. Der Auftragnehmer bestätigt, dass ihm und seinen Mitarbeitern, die mit Auftraggeber-Daten umgehen, die Vorschriften der DS-GVO und die sonstigen einschlägigen Datenschutzvorschriften bekannt sind und beachtet werden.
(2) Der Auftragnehmer führt für die Verarbeitung von Daten ein **Verzeichnis** der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.
(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgen-abschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.
(4) Die Wahrung des Fernmeldegeheimnisses entsprechend §88 TKG muss vom Auftragnehmer gewährleistet werden. Dazu muss der Auftragnehmer alle Personen, die auftragsgemäß auf Daten des Auftraggebers mittels Mittel der Telekommunikation wie Telefon oder E-Mail zugreifen können, auf das Fernmeldegeheimnis verpflichten und über die sich daraus ergebenden besonderen Geheimhaltungspflichten belehren.

(5) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
(6) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit

Björn Leineweber, Rechtsanwalt und zertifizierter Datenschutzbeauftragter, von der BELA Datenschutz UG, Ruhrtalstr. 67, 45239 Essen, leineweber@datenschutz-ruhr.de, www.datenschutz-ruhr.de

benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(7) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.
(8) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
(9) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
(11) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.
(12) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsdatenverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(13) 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 beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

§ 5 Allgemeine Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.
(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
(3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.
(4) Dem Auftraggeber obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen
(5) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 6 Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies auf Verlangen nach.
(2) Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.
(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.
(4) Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.
(5) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.
(6) Bei einer Leistungserbringung in einem sicheren Drittstaat wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen Vorgaben der DS-GVO wird durch den Auftragnehmer gewährleistet.
(7) Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

(8) Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 7 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe in **Anlage 1** dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) 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.

(4) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

§ 8 Mitteilungs- und Unterstützungspflichten des Auftragnehmers zur Sicherheit personenbezogener Daten

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen. Insbesondere ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich über die Verletzung des Schutzes personenbezogener Daten („Datenpannen“) gemäß Art. 33 Abs. 2 DS-GVO zu informieren.

(2) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 9 Berichtigung, Einschränkung, Übertragbarkeit und Löschung von Daten

(1) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erfüllung von Ansprüchen Betroffener auf Auskunft, Berichtigung, Sperrung, Übertragbarkeit oder Löschung von Auftraggeber-Daten auf erstes Anfordern im Rahmen des Zumutbaren zu unterstützen. Insbesondere wird der Auftragnehmer dem Auftraggeber unverzüglich, längstens aber innerhalb von fünf Werktagen Informationen über die gespeicherten Auftraggeber-Daten (auch soweit sie sich auf den Speicherungszweck beziehen), die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen.
(3) Der Auftragnehmer ist verpflichtet, Auftraggeber-Daten auf Weisung des Auftraggebers unverzüglich, spätestens aber innerhalb einer Frist von fünf Werktagen, zu berichtigen, zu löschen zu sperren oder zu übertragen (Artt. 16 - 20 DS-GVO). Der Auftragnehmer wird dem Auftraggeber die weisungsgemäße Berichtigung, Sperrung und Löschung jeweils auf Verlangen schriftlich bestätigen.
(4) Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

§ 10 Auskunft an Dritte

Soweit der Auftragnehmer aufgrund gesetzlicher Bestimmungen Dritten Auskunft über Auftraggeber-Daten erteilen muss, ist der Auftragnehmer verpflichtet, den Auftraggeber rechtzeitig vor Auskunftserteilung über Empfänger, Zeitpunkt und Inhalt der zu erteilenden Auskunft und deren Rechtsgrundlage schriftlich oder in Textform zu informieren.

§ 11 Rückgabe und Löschung überlassener Daten und Datenträger

(1) Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch Auftraggeber-Daten enthalten, an den Auftraggeber zurückzugeben oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.
(2) Über eine Löschung bzw. Vernichtung von Auftraggeber-Daten hat der Auftragnehmer ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung vorzulegen ist.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben

§ 12 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person

an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 13 Kontrollrechte

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung der diesem nach dem vorliegenden Vertrag gestatteten Kontrollen erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.
(4) Der Nachweis der Umsetzung technischer und organisatorischer Maßnahmen nach **Anlage 1** kann anstatt einer Vor-Ort-Kontrolle auch durch den Nachweis der Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren), einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) oder genehmigte Zertifizierungsverfahren gemäß Art. 42 DS-GVO erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 1** zu diesem Vertrag zu überzeugen.

§ 14 Subunternehmer (weitere Auftragsdatenverarbeiter)

(1) Der Auftraggeber stimmt hiermit der Begründung der Unterauftragsverhältnisse gemäß **Anlage 2** zu. Jeder Wechsel oder Austausch eines Unterauftragnehmers bedarf der Zustimmung durch den Auftraggeber; **Anlage 2** ist dann entsprechend zu aktualisieren.
(2) Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer muss der Auftragnehmer nur dann die Zustimmung des Auftraggebers einholen, wenn es sich um atypische Dienstleister handelt, die nicht regelmäßig im Rahmen der Leistungserbringung zwischen Auftragnehmer und Auftraggeber relevant werden oder die nicht im Rahmen einer vertraglichen Vereinbarung genannt wurden. Eine entsprechende Zustimmung darf nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden.
(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
(4) Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des Art. 28 DS-GVO und Art. 32 DS-GVO

beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

(5) Keiner Zustimmung bedarf die Einschaltung von Subunternehmern, bei denen der Subunternehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung in Anspruch nimmt, auch wenn dabei ein Zugriff auf die Auftraggeber-Daten nicht ausgeschlossen werden kann; dazu zählen insbesondere Transportleistungen von Post- oder Kurierdiensten sowie Geldtransportdienstleistungen, Telekommunikationsdienste, Bewachungsdienste und Reinigungsdienste, nicht aber Prüfungs- und Wartungsleistungen. Der Auftragnehmer wird mit solchen Subunternehmern branchenübliche Geheimhaltungsvereinbarungen treffen.

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 5 eingesetzt werden sollen.

§ 15 Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
   a. er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
   b. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
   c. er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

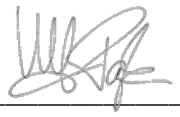
(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
   a. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
   b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 16 Informationspflichten, Schriftformklausel, Rechtswahl

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

(2) Änderungen und Ergänzungen dieser 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.
(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
(4) Es gilt deutsches Recht.



Papke Media GmbH & Co.KG,

Ulf Papke, Geschäftsführer

ANLAGE 1

Technische und organisatorische Maßnahmen

der Firma

Terminpilot.de,
betrieben durch die Papke Media GmbH & Co KG,
Johann-Krane-Weg 8,
48149 Münster

A. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- ☒ Alarmanlage
- ☐ Automatisches Zugangskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Lichtschranken / Bewegungsmelder / Kontaktunterbrecher
- ☒ Wachpersonal
- ☐ Absicherung von Gebäudeschächten
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Sicherheitsschlösser
- ☐ Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen:

- ☒ Berechtigungsvergabeverfahren vorhanden
- ☒ Passwortvergabe mit verbindlichen Regeln:
  - ☒ Zeichen-Mix
  - ☒ Mind. 8 Zeichen
  - ☒ Regelmäßiger Passwortwechsel ( )
  - ☒ Passworthistorie
  - ☒ Keine Gruppenpasswörter
  - ☒ Passwortrücksetzungsverfahren
  - ☒ Aufbewahrung Admin-Passwort
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Gehäuseverriegelungen
- ☐ Einhaltung Need-to-Know-Prinzip
- ☒ Verschlüsselung auf Website
- ☒ Benutzerprofile
- ☐ Authentifikation mit biometrischen Verfahren
- ☒ Protokollierung des Systemzugangs bzw. der Systemzugriffsrechte
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☐ Einsatz von VPN-Technologie
- ☒ Vertragliche und technische Regelung Einbindung Drittsysteme auf Website
- ☐ Verbot externer Schnittstellen (USB)

☒ Regelung zur Erstellung und Aufbewahrung von Passwörtern für Kundenkonten

☒ Server nur extern, AVV abgeschlossen, Kundenkonten werden nicht gespeichert, Unterteilung Admin- und Leserechte

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☒ IT-Berechtigungskonzept

☐ Verwaltung der Rechte durch Systemadministrator; differenzierte Berechtigungen

☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☐ Auswertung von Logs

☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☒ Sichere Aufbewahrung von Datenträgern

☒ physische Löschung von Datenträgern vor Wiederverwendung

☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☒ Verschlüsselung von Datenträgern

☒ Verschlüsselung von Smartphones, Laptops

☐ Verschlüsselung mobile Daten

☒ Verschlüsselung Back-Up

☐ Regelung von Datenwiederherstellung aus Backup

☒ Bei Hosting: Auftraggeber muss jeden einzelnen Wartungsvorgang veranlassen

4. Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☐ Logische Mandanten-/Kundentrennung (softwareseitig)

☐ Berechtigungskonzept zur Trennung der Daten des Kunden im System, sowie Festlegung spezieller Rechte bzgl. des Datenzugriffs (Lesen, Schreiben, Ändern) pro Benutzer

☒ Funktionstrennung (z.B. unterschiedliche Verarbeitung Buchhaltung und Kunden)

☐ Festlegung Datenbankrechte

☒ Trennung von Produktiv- und Testsystem

☐ Trennung von Kundendaten im Hinblick auf Daten anderer Kunden aufgrund eines Berechtigungskonzepts

☒ Trennung von Lese- und Schreibzugriff

B. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

- ☐ Pseudonymisierung (Geschäfts-) Kundendaten
- ☒ Pseudoymisierung Userdaten / Privatkunden
- ☒ Pseudonymisierung IP-Adressen (bei etwaiger Weitergabe / Weiterleitung an Dritte zu Analyse, Marketing, Tracking o.ä.)
- ☐ Pseudonymisierung Mitarbeiterdaten
- ☐ Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☒ Datenminimierung, im Übrigen Pseudonymisierung auch bei Hoster

C. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☐ VPN-Tunnel
  - ☐ Berechtigungskonzept
  - ☐ Identifizierung / Authentifizierung
  - ☐ Logs
  - ☐ Sperre bei Verstoß
- ☒ Beim physischen Transport:
  - ☐ sichere Transportbehälter
  - ☐ Datenträgerliste
  - ☒ verschlüsselter Datenträger
  - ☐ Sorgfältige Auswahl Transportpersonal
  - ☐ Empfangsbestätigung
  - ☐ Rückgabedokumentation
- ☒ E-Mail-Verschlüsselung
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Verschlüsselung Datenübermtittlung

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten

☒ Protokollierung der Administratortätigkeiten

☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden.

☒ Plausibilitätskontrolle bei Dateneingabe bzw. -änderung

D. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und die eine rasche Wiederherstellbarkeit gemäß Art. 32 Abs. 1 lit c. DSGVO gewährleisten

☒ Unterbrechungsfreie Stromversorgung (USV)

☐ Klimaanlage in Serverräumen

☒ Einsatz einer Sicherheitssoftware, wie:
- ☒ Virenscanner
- ☒ Firewalls
- ☒ SPAM Filter
- ☐ Verschlüsselungsprogramme

☒ Cloud-Speicher
- ☒ in Europa
- ☐ vertragliche Regelung liegt vor

☒ Verfügbarkeitskontrolle bei Hosting-Unternehmen gewährleistet

E. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs.1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

1. Datenschutzmanagement

☒ Technische und organisatorische Maßnahmen durch Datenschutzbeauftragten überprüft

☒ Datenschutzfreundliche Voreinstellung (nur solche Daten, die für den jeweiligen Zweck erforderlich sind)

☒ Selbstverpflichtung zur regelmäßigen Überprüfung des angemessenen Schutzniveaus

☒ Selbstverpflichtung zur Überprüfung neuer Verfahren

☒ Selbstverpflichtung zur regelmäßigen Löschung von Daten, die aus der Speicherfrist fallen

☒ Zur Kenntnis genommen, dass bei Datenschutzpanne sofortige Kontaktaufnahme zum Datenschutzbeauftragten (soweit vorhanden) und zur Aufsichtsbehörde erforderlich (Maximalfrist 72 Stunden!)

2. Auftragskontrolle

☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)

☒ Auftragnehmer hat Datenschutzbeauftragten bestellt (soweit erforderlich), Hinweis:

☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

☒ Weitergabe von Datenschutz-Informationen an Mitarbeiter in Form von
- ☒ Merkblättern
- ☐ Schulungen
- ☐ Zugriff von mit der Verarbeitung von Kundendaten betrauten Mitarbeitern auf Übersicht der sie betreffenden Schutz-maßnahmen

☐ vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

☒ Betriebsvereinbarung Mitarbeiter
- ☒ E-Mail-Nutzung (nicht privat)
- ☐ E-Mail Nutzung (auch privat, aber mit Einwilligung Verarbeitung Arbeitgeber)
- ☐ Nutzung eigener Geräte
- ☐ Aufbewahrung, Sicherung Firmengeräte

F. Datenverarbeitung außerhalb EU bzw. EU-Schutzniveau

☒ Keine Datenspeicherung außerhalb EU

☒ Datenspeicherung wenn EU, mit Gewährleistung Sicherheit (z.B. Privacy Shield) und Vertragsgestaltung (AV-Vertrag)

☒ Einsatz Tracking-Tools Website mit Hinweis an Nutzer und Sicherstellung Datenschutz aufgrund Vertrag mit Anbieter

☒ Einsatz Analyse-Tools Website mit Hinweis an Nutzer und Sicherstellung Datenschutz aufgrund Vertrag mit Anbieter

17.05.2018
Datum

Ulf Papke (Geschäftsführer)
Verantwortlicher für die Erstellung (in Druckbuchstaben)

Unterschrift des Verantwortlichen

Anlage 2: Unterauftragnehmer

Unterauftragnehmer	**Tätigkeiten**	**Zweck**	**Kategorien von Daten**	**Betroffene**
POKAmax GmH	Postkartenversand	Vertragserfüllung, Erbringung vereinbarter Leistungen	Adressdaten	Kunden, Endkunden
CM Telecom Germany GmbH	SMS-Versand	Versand von SMS über das Software-System	Kontaktdaten, Telefonnummern, Namen	Kunden, Endkunden
Hetzner Online GmbH	Server, IT, Cloud	Speicherung von Daten des IT-Systems	Alle Daten des IT-Systems, inklusive Daten von Webseiten-Besuchern wie IP-Adressen	Kunden, Endkunden, Interessenten, Website-Nutzer
Klick-Tipp Ltd., 15 Cambridge Court, 210 Shepherd's Bush Road, London W6 7NJ, Vereinigtes Königreich	Newsletterversand	Marketing	E-Mail-Adressen, Namen	Kunden, Mitarbeiter der Kunden (Mail-Empfänger)
Zammad GmbH	Helpdesk, Ticketsystem	Projektmanagement, Kundenbetreuung	E-Mail-Adressen, Namen, Kundendaten	Kunden, ~~Endkunden~~
Google	Business-Suite, Analytics	Office-Anwendung, Analyse von Websitenutzung durch Websitenutzer	Kundendaten (Office), IP-Daten (Analytics) – jedoch mit IP-Anonymisierung	Kunden, Website-Nutzer
BELA Datenschutz UG	Datenschutzbeauftragter	Datenschutz	Auftragnehmerdaten	Auftragnehmer