Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

zwischen

der Lindemann audiotechnik GmbH, Am Anger 4, DE-82237 Wörthsee, Kundennr. 655584

- **Auftraggeber** oder **Verantwortlicher** -

und

der Timme Hosting GmbH & Co. KG, gesetzlich vertreten durch die persönlich haftende Gesellschafterin: Timme Hosting Verwaltungs GmbH, diese gesetzlich vertreten durch den Geschäftsführer: Falko Timme, Ovelgönner Weg 43, 21335 Lüneburg, Deutschland,

- **Auftragnehmer** oder **Auftragsverarbeiter** -

Vorbemerkungen

Der Auftragnehmer erbringt Hosting-Leistungen, die der Auftraggeber auf Grundlage eines gesonderten Vertrages oder mehrerer gesonderter Verträge in Anspruch nimmt. Bei dem gesonderten Vertrag oder den gesonderten Verträgen handelt es sich um alle laufenden, auch künftigen Verträge zwischen den Parteien über die Erbringung von Hosting-Leistungen durch den Auftragnehmer für den Auftraggeber.

Der gesonderte Vertrag oder die gesonderten Verträge werden nachfolgend insgesamt Hauptvertrag genannt. Der Hauptvertrag sieht unter anderem eine Verarbeitung von Daten durch den Auftragnehmer im Auftrag des Auftraggebers vor. Bei diesen Daten kann es sich auch um personenbezogene Daten handeln. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (Betroffener) beziehen. Soweit die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers betroffen ist (Auftragsverarbeitung), ergänzt dieser Vertrag den Hauptvertrag. Insoweit gehen abweichende Regelungen in diesem Vertrag den Regelungen des Hauptvertrages vor. Bei der Verarbeitung personenbezogener Daten beachten die Parteien die datenschutzrechtlichen Vorschriften, insbesondere die Vorschriften der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

Die DSGVO gilt ab dem 25. Mai 2018. Sofern die Parteien bereits eine Vereinbarung über die Auftragsdatenverarbeitung (ADV) geschlossen haben, ersetzt dieser Vertrag die ADV ab Geltung der DSGVO.

§ 1 Gegenstand und Dauer

(1) Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag. Namentlich handelt es sich dabei um Hosting-Leistungen wie die Bereitstellung und das Verwalten von physischen oder virtuellen Servern bzw. Teilen davon (Managed Server / Managed Hosting / Shared Hosting / Cloud). Die personenbezogenen Daten, die gemäß diesem Vertrag verarbeitet werden, sind solche, die der Auftragnehmer im Auftrag des Auftraggebers erhoben hat, oder die dem Auftragnehmer vom Auftraggeber zur Auftragsverarbeitung übermittelt worden sind. Der Auftraggeber gewährleistet, dass aus den für ihn zu erhebenden oder von ihm übermittelten Daten nicht die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Ebenso handelt es sich nicht um Daten über strafrechtliche Verurteilungen oder Straftaten und nicht um genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, um Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer solchen Person.

(2) Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages. Nach Abschluss der Erbringung der Verarbeitungsleistungen wird der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder zurückgeben, sofern nicht nach den gesetzlichen Vorschriften eine Verpflichtung zur Speicherung dieser Daten besteht. Die Rückgabe ist beschränkt auf Datenträger, die der Auftraggeber dem Auftragnehmer überlassen hat. Auf Verlangen wird der Auftragnehmer dem Auftraggeber die Löschung noch einmal gesondert bestätigen.

§ 2 Inhalt des Auftrags

(1) Die Art und der Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag. Namentlich kann der Auftragnehmer bei der Server-Verwaltung mit den Daten in Berührung kommen, die auf den zur Erbringung der Hosting-Leistungen für den Kunden eingesetzten Servern verarbeitet werden. Bei den personenbezogenen Daten, die auf den Servern verarbeitet werden, handelt es sich um (Art der Daten):

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
- Protokolldaten
- Vertragsabrechnungs- und Zahlungsdaten

Der Auftragnehmer wird die Daten zu keinen anderen als den vertraglichen Zwecken verarbeiten. Insbesondere wird er die Daten nicht außerhalb des Auftrags an Dritte übermitteln. Kopien wird der Auftragnehmer nur für die auftragsgemäße Verarbeitung der Daten herstellen (bspw. Sicherheitskopie).

(2) Von der Auftragsverarbeitung sind die Daten folgender Personen betroffen (Kategorien der Personen):

- Kunden und Interessenten des Auftraggebers
- Mitarbeiter und Lieferanten des Auftraggebers

(3) Der Auftraggeber bleibt für die Verarbeitung personenbezogener Daten, die in seinem Auftrag erfolgt, allein verantwortlich. Der Auftragnehmer wird diese Daten daher nur auf Weisung des Auftraggebers verarbeiten, sofern er nicht nach den gesetzlichen Vorschriften zu einer anderweitigen Verarbeitung verpflichtet ist. Dies teilt der Auftragnehmer dem Auftraggeber vor der anderweitigen Verarbeitung jedoch mit, sofern ihm das Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Verantwortlichkeit des Auftraggebers bezieht sich insbesondere darauf, dass die vertrags- und weisungsgemäße Datenverarbeitung rechtmäßig ist, die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden und deren Einhaltung nachgewiesen werden kann.

(4) Die Weisungen werden anfänglich durch den Hauptvertrag und diesen Vertrag festgelegt und dokumentiert. Die anfänglichen Weisungen kann der Auftraggeber später durch gesonderte Weisung (Einzelweisung) ändern, ersetzen oder ergänzen. Die Einzelweisung muss sich im Rahmen des Auftrags bewegen und ist ebenfalls zu dokumentieren. Wird eine Einzelweisung wegen besonderer Dringlichkeit mündlich erteilt, ist sie unverzüglich in dokumentierter Form zu bestätigen. Dabei meint Weisung jede Vorgabe, die sich auf einen bestimmten datenschutzmäßigen Umgang mit den nach diesem Vertrag im Auftrag verarbeiteten Daten bezieht (bspw. Löschung, Anonymisierung und Berichtigung von Daten oder die Einschränkung der Datenverarbeitung).

(5) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die gesetzlichen Vorschriften verstößt, wird er den Auftraggeber unverzüglich informieren. Insoweit ist der Auftragnehmer berechtigt, die Umsetzung der Weisung solange auszusetzen, bis sie vom Auftraggeber in dokumentierter Form geändert oder bestätigt wird. Bestimmt der Auftragnehmer die Zwecke und Mittel der Verarbeitung unter Verstoß gegen die Weisungen des Auftraggebers selbst, gilt er in Bezug auf diese Verarbeitung als verantwortlich.

(6) Die Auftragsverarbeitung erfolgt in den Mitgliedsstaaten der Europäischen Union (EU). Die Übermittlung der verarbeiteten Daten in ein Drittland bedarf der Zustimmung durch den Auftraggeber, die nur aus wichtigem Grund verweigert werden darf. Einen Grund für die Verweigerung stellt es insbesondere dar, wenn das Drittland kein angemessenes Schutzniveau bietet oder sonst die gesetzlichen Voraussetzungen für eine Übermittlung der Daten in das jeweilige Land nicht gegeben sind. Zweifel gehen insoweit zu Lasten des Auftragnehmers.

(7) Der Auftraggeber wird in Zusammenhang mit der Auftragsverarbeitung niemanden einer ausschließlich auf einer automatisierten Verarbeitung einschließlich Profiling beruhenden Entscheidung unterwerfen, die dem Betroffenen gegenüber rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt. Ebenso lässt der Auftraggeber die Daten nicht im Auftrag für ein Angebot verarbeiten, das einem Kind direkt gemacht wird (bspw. für speziell an Kinder gerichtete Dienste).

§ 3 Ansprechpartner

(1)Der Auftraggeber kann dem Auftragnehmer einen Ansprechpartner für die Durchführung dieses Vertrages benennen. Die Benennung hat in dokumentierter Form zu erfolgen. Bis dahin gilt als Ansprechpartner die Person, die diesen Vertrag für den Auftraggeber geschlossen hat. Der Ansprechpartner ist zugleich die Person, die gegenüber dem Auftragnehmer berechtigt ist, datenschutzrechtliche Weisungen nach diesem Vertrag zu erteilen.

(2) Ansprechpartner beim Auftragnehmer für die Durchführung dieses Vertrages ist:

Falko Timme, erreichbar über die Anschrift des Auftragnehmers, Telefon: +49 (0)4131 227810, Telefax: +49 (0)4131 2278178, E-Mail: support@timmehosting.de

Der Ansprechpartner ist zugleich die Person, die gegenüber dem Auftraggeber berechtigt ist, datenschutzrechtliche Weisungen nach diesem Vertrag zu empfangen.

(3) Die Parteien können ihre Ansprechpartner jederzeit ändern. Es können mehrere Ansprechpartner benannt werden, die jeweils einzeln weisungs- bzw. empfangsberechtigt sind. Ist der Ansprechpartner einer Partei mehr als nur vorübergehend nicht erreichbar, hat die Partei den Ansprechpartner jedenfalls für die Dauer der Nichterreichbarkeit zu ändern. Die Änderung eines Ansprechpartners hat in dokumentierter Form zu erfolgen.

(4) Ist eine Partei nicht in der EU niedergelassen, hat sie schriftlich einen Vertreter zu benennen. Dieser Vertreter vertritt die Partei in Bezug auf die ihr nach den datenschutzrechtlichen Vorschriften in der EU obliegenden Pflichten. Dazu muss der Vertreter in einem der Mitgliedstaaten der EU niedergelassen sein, in dem sich die von der Auftragsverarbeitung betroffenen Personen befinden. Ein solcher Vertreter ist in diesem Vertrag als Ansprechpartner zu benennen. Bei der Benennung ist zu vermerken, dass es sich um einen Vertreter im Sinne der DSGVO handelt.

§ 4 Datenschutzbeauftragter

(1) Eine Pflicht zur Benennung eines Datenschutzbeauftragten begründet dieser Vertrag nicht. Den Parteien ist jedoch bekannt, dass ein Datenschutzbeauftragter nach den gesetzlichen Vorschriften unter anderem zu benennen ist, wenn a) die Kerntätigkeit der jeweiligen Partei in der Durchführung von Verarbeitungsvorgängen besteht, welche eine umfangreiche regelmäßige und systematische Überwachung erforderlich machen, wenn b) in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, oder wenn c) die Daten geschäftsmäßig zum Zwecke der Übermittlung oder der Markt- oder Meinungsforschung verarbeitet werden.

(2)Soweit der Auftraggeber einen Datenschutzbeauftragten benannt hat, teilt er dies dem Auftragnehmer in dokumentierter Form mit.

(3) Als Datenschutzbeauftragten hat der Auftragnehmer benannt:

Rechtsanwalt Daniel Raimer, erreichbar über die Kanzlei Daniel Raimer, Ernst-Gnoß-Str. 22, 40219 Düsseldorf, Deutschland, Telefon: +49 (0)211 4167 4600, Telefax: +49 (0)211 4167 4601, E-Mail: office@kanzlei-raimer.com

(4) Die Regelung zur Änderung des Ansprechpartners gilt für den Datenschutzbeauftragten entsprechend. Der Ansprechpartner kann zugleich der Datenschutzbeauftragte sein. Bestellt eine Partei nachträglich einen Datenschutzbeauftragten, teilt sie dies der anderen Partei unverzüglich in dokumentierter Form mit. Der Datenschutzbeauftragte des Auftraggebers ist zur Erteilung, der Datenschutzbeauftragte des Auftragnehmers zum Empfang von Weisungen berechtigt.

(5) Der Datenschutzbeauftragte wird von der jeweiligen Partei in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden und die Einhaltung der datenschutzrechtlichen Vorschriften überwachen. Die Parteien können den Datenschutzbeauftragten der jeweils anderen Partei zu allen Fragen bei der Verarbeitung von personenbezogenen Daten gemäß diesem Vertrag zu Rate ziehen.

§ 5 Rechte und Pflichten

(1) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung von personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dies gilt insbesondere für die dem Auftragnehmer unterstellten Personen (Mitarbeiter), die Zugang zu den im Auftrag verarbeiteten Daten haben. Zugleich stellt der Auftragnehmer sicher, dass seine Mitarbeiter diese Daten nur nach den Weisungen des Auftraggebers verarbeiten, sofern sie nicht nach den gesetzlichen Vorschriften zu einer anderweitigen Verarbeitung verpflichtet sind. Die Pflicht zur Vertraulichkeit bzw. Verschwiegenheit gilt auch über das Ende des Auftrags hinaus.

(2) Der Auftragnehmer unterstützt den Auftraggeber dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte nachzukommen, die den Betroffenen gegenüber dem Auftraggeber gesetzlich zustehen. Wendet ein Betroffener sich an den Auftragnehmer, leitet dieser den Antrag des Betroffenen unverzüglich an den Auftraggeber weiter. Ohne eine Weisung des Auftraggebers wird der Auftragnehmer Betroffenenanträge nicht selbst beantworten. Außerdem unterstützen die Parteien sich unter Berücksichtigung der Art der Auftragsverarbeitung und der ihnen zur Verfügung stehenden Informationen bei der Einhaltung ihrer gesetzlichen Pflichten zum Datenschutz. Namentlich gilt dies für die Pflicht, die Sicherheit der Verarbeitung zu gewährleisten, Verletzungen des Datenschutzes an die Aufsichtsbehörde zu melden sowie die Betroffenen davon zu benachrichtigen, eine Datenschutz-Folgeabschätzung durchzuführen, die Aufsichtsbehörde zu konsultieren und ein Verzeichnis der Tätigkeiten bei der Auftragsverarbeitung zu erstellen.

(3) Die Parteien stellen sich auf Verlangen alle erforderlichen Informationen zum Nachweis der

Einhaltung der in diesem Vertrag zum Datenschutz niedergelegten Pflichten zur Verfügung. Das gleiche gilt für die Informationen, die zum Nachweis der Einhaltung der in den gesetzlichen Vorschriften über die Auftragsverarbeitung niedergelegten Pflichten erforderlich sind. Darüber hinaus ermöglicht der Auftragnehmer Überprüfungen einschließlich Inspektionen, die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden. Der Auftragnehmer kann gegen einen Prüfer, der mit ihm in Wettbewerb steht, Einspruch erheben. Für Inspektionen, die vor Ort beim Auftragnehmer durchgeführt werden müssen, vereinbart der Auftraggeber rechtzeitig vorher einen Termin. Vor der Überprüfung hat sich der Auftraggeber bzw. Prüfer zur Vertraulichkeit zu verpflichten. Dies gilt nicht, wenn ausgeschlossen ist, dass der Auftraggeber bzw. Prüfer mit anderen als den nach diesem Vertrag verarbeiteten Informationen in Berührung kommt. Soweit erforderlich, trägt der Auftragnehmer zu der Überprüfung bei. Der Nachweis von Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch durch Testate oder Berichte einer unabhängigen Stelle (bspw. Wirtschaftsprüfer oder Datenschutzauditor) erbracht werden. Das gleiche gilt für genehmigte oder sonst geeignete Zertifizierungen durch eine unabhängige Stelle.

(4) Wird dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt, die im Auftrag verarbeitet werden, meldet er dies unverzüglich dem Auftraggeber. Das gleiche gilt, wenn die im Auftrag verarbeiteten Daten beim Auftragnehmer von einer Pfändung oder Beschlagnahme, von einem Insolvenzverfahren oder von ähnlichen Maßnahmen betroffen sind. Bei Gefahr im Verzug ist der Auftragnehmer berechtigt und verpflichtet, darauf hinzuweisen, dass die Verantwortung für die betroffenen Daten beim Auftraggeber liegt. Die Parteien werden angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Auswirkungen, insbesondere auch für die betroffenen Personen, ergreifen und sich bei der Dokumentation unterstützen. Auch über Maßnahmen, die eine Aufsichtsbehörde in Zusammenhang mit der Auftragsverarbeitung ergreift, werden die Parteien sich informieren, soweit dies zulässig ist.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und den Schutz der Rechte der Betroffenen gewährleistet. Dabei berücksichtigt der Auftragnehmer den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Auftragsverarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Insgesamt wird der Auftragnehmer durch seine technischen und organisatorischen Maßnahmen ein dem Risiko angemessenes Schutzniveau gewährleisten. Diese Maßnahmen schließen unter anderem ein: a) die Verschlüsselung personenbezogener Daten, b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen sowie c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Die für den Auftraggeber verarbeiteten Daten werden nach Möglichkeit technisch und organisatorisch von anderen Daten getrennt.

(2) Im Einzelnen können die ergriffenen Maßnahmen dem Anhang zu diesem Vertrag entnommen werden. Der Auftraggeber erkennt diese Maßnahmen als nach dem Stand der Technik ausreichend an. Die Einhaltung und die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung werden vom Auftragnehmer regelmäßig überprüft und erforderlichenfalls aktualisiert. Bei der Überprüfung wird der Auftragnehmer die Risiken berücksichtigen, die mit der Verarbeitung, insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden, verbunden sind. Bei der Aktualisierung wird der Auftragnehmer das nach diesem Vertrag gewährleistete Schutzniveau nicht unterschreiten. Wesentliche Änderungen, die sich durch die Aktualisierung der Maßnahmen ergeben, wird der Auftragnehmer dokumentieren.

§ 7 Unterauftragnehmer

(1) Der Auftragnehmer nimmt zurzeit folgende weitere Auftragsverarbeiter (Unterauftragnehmer) in Anspruch:

keine

Soweit ein Unterauftragnehmer die Daten in einem Drittland verarbeitet, ist dies zu vermerken. Zugleich ist anzugeben, woraus das angemessenes Schutzniveau für die Datenverarbeitung durch den Unterauftragnehmer folgt. Insoweit stimmt der Auftraggeber der Datenübermittlung in das Drittland zu.

(2) Der Auftragnehmer ist berechtigt, weitere Unterauftragnehmer hinzuzuziehen oder die in Anspruch genommenen Unterauftragnehmer durch andere Unterauftragnehmer zu ersetzen. Der Auftragnehmer informiert den Auftraggeber jedoch vorab über die beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung. Dadurch erhält der Auftraggeber die Möglichkeit, gegen die beabsichtigte Änderung Einspruch zu erheben. Der Einspruch ist innerhalb eines Ausschlussfrist von sechs Wochen ab Erhalt der Information über die beabsichtigte Änderung zu erheben. Sowohl die Information als auch der Einspruch bedürfen der Textform, wobei der Auftragnehmer den Auftraggeber in der Information noch einmal auf die Ausschlussfrist hinweisen wird. Erhebt der Auftraggeber ohne wichtigen Grund Einspruch gegen die Änderung, ist der Auftragnehmer mit einer Frist von sechs Wochen zur vorzeitigen Kündigung sowohl dieses Vertrages als auch des Hauptvertrages berechtigt.

(3) Der Auftragnehmer wird den Unterauftragnehmern im Wege eines Vertrags dieselben Datenschutzpflichten auferlegen, die in diesem Vertrag zwischen den Parteien festgelegt sind. Insbesondere muss der Unterauftragnehmer geeignete technische und organisatorische Maßnahmen so durchführen, dass die Verarbeitung entsprechend den datenschutzrechtlichen Anforderungen erfolgt. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so

haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des jeweiligen Unterauftragnehmers. Der Auftragnehmer wird im Auftrag des Auftraggebers verarbeitete Daten erst an einen Unterauftragnehmer übermitteln, wenn dafür die Voraussetzungen nach diesem Vertrag gegeben sind.

(4) Nicht als Unterauftragnehmer zu verstehen sind Dritte, von denen der Auftragnehmer Leistungen als Nebenleistung zur Unterstützung bei der Vertragsdurchführung in Anspruch nimmt. Dazu zählen etwa Telekommunikations-, Post-, Wartungs- und Prüfungsdienste. Auch insoweit wird der Auftragnehmer jedoch Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (bspw. Vertraulichkeitsverpflichtung, Überwachung oder Verschlüsselung).

§ 8 Kosten

(1) Der Auftragnehmer erbringt die Umsetzung der durch den Hauptvertrag festgelegten Weisungen und sorgt für die Einhaltung der allgemeinen und technischen und organisatorischen Maßnahmen, ohne dem Auftraggeber dafür Kosten nach diesem Vertrag zu berechnen. Insoweit sind die Tätigkeiten des Auftragnehmers also schon durch die Vergütung nach Maßgabe des Hauptvertrages abgegolten. Das gleiche gilt für Einzelweisungen, die der Auftraggeber über das Verarbeitungssystem des Auftragnehmers nach dem Hauptvertrag selbst umsetzen kann und auch selbst umsetzt (bspw. über ein Webinterface).

(2) Dagegen fallen die Kosten für die Umsetzung von Einzelweisungen und sonstiger Verlangen dem Auftraggeber zur Last. Dies gilt insbesondere für die Unterstützung bei der Beantwortung von Betroffenenanträgen und bei der Einhaltung sonstiger Pflichten, die dem Auftraggeber obliegen, für die Rückgabe und Vernichtung von Daten, soweit diese über eine Löschung im System des Auftragnehmers hinausgeht, für die Zurverfügungstellung von Informationen, soweit diese nicht überwiegend im Interesse des Auftragnehmers liegt, und für das Ermöglichen und Beitragen zu Prüfungen einschließlich Inspektionen.

(3) Auf Verlangen wird der Auftragnehmer dem Auftraggeber vorab eine Kostenschätzung geben. Zu den Kosten gehört auch eine angemessene Vergütung des Arbeitsaufwands. Im Zweifel handelt es sich dabei um individuellen Support, der gemäß der Preisliste (s. https://timmehosting.de/preisliste-zusatzprodukte-und-zusatzdienstleistungen) des Auftragnehmers zu vergüten ist. Abweichende Kostenregelungen aus dem Hauptvertrag oder der Preisliste, die sich auf bestimmte datenschutzrechtliche Maßnahmen beziehen, gehen dieser Kostenregelung vor. Ebenso fallen die Kosten für Maßnahmen, deren Erforderlichkeit eine Partei schuldhaft verursacht hat, dieser Partei zur Last. Ein Mitverschulden der jeweils anderen Partei ist jedoch zu berücksichtigen.

§ 9 Schlussbestimmungen

(1) Der Vertrag bleibt auch bei rechtlicher Unwirksamkeit einzelner Regelungen in seinen übrigen Teilen verbindlich. An die Stelle der unwirksamen Regelungen treten die gesetzlichen Bestimmungen. Der Vertrag gilt nicht für die Verarbeitung von Daten ohne Personenbezug. Dies auch dann nicht, wenn sie von den Parteien versehentlich oder rechtsirrig als personenbezogen eingestuft worden sind. Insoweit gelten allein die Regelungen des Hauptvertrages.

(2) Es findet das Recht der Bundesrepublik Deutschland Anwendung. Eine Regelung zum Gerichtsstand und zur Haftungsbeschränkung im Hauptvertrag gilt auch für diesen Vertrag, ohne dass dadurch die gesetzlichen Rechte der Betroffenen beschränkt werden.

(3) Änderungen, Ergänzungen und die Aufhebung dieses Vertrages müssen in dokumentierter Form erfolgen. Dokumentierte Form im Sinne dieses Vertrages meint mindestens die Textform. Auf Verlangen einer Partei ist eine in Textform abgegebene Erklärung schriftlich zu bestätigen.

Anhang
Technische und organisatorische Maßnahmen

_____, den _____

Lüneburg, den 08.12.2020

Auftraggeber durch:

Auftragnehmer durch:

_____

Vor- und Nachname

Falko Timme

Vor- und Nachname

_____

Unterschrift(*) und ggf. Stempel

Unterschrift(*) und ggf. Stempel

* Der Vertrag ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

Anhang

Technische und organisatorische Maßnahmen

der **Timme Hosting GmbH & Co. KG**, gesetzlich vertreten durch die persönlich haftende Gesellschafterin: Timme Hosting Verwaltungs GmbH, diese gesetzlich vertreten durch den Geschäftsführer: Falko Timme, Ovelgönner Weg 43, 21335 Lüneburg, Deutschland,

- **Timme Hosting** -

bei der Verarbeitung personenbezogener Daten.

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer Daten trifft Timme Hosting geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen werden so durchgeführt, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen, insbesondere den Vorschriften der Datenschutzgrundverordnung (DSGVO), erfolgt und schließen Folgendes ein:

I. Verschlüsselung

Timme Hosting greift auf die Geräte und Anlagen, auf denen personenbezogene Daten verarbeitet werden (Verarbeitungssysteme), nur über verschlüsselte Verbindungen zu. Für die Verschlüsselung der Verbindung wird die Transport Layer Security (TLS, früher: SSL) eingesetzt. Die über die Verbindung transportierten Daten werden nach dem Advanced Encryption Standard (AES) verschlüsselt. Als Schlüssellänge werden wenigstens 256 Bit verwendet (AES-256). Bei einem Web-Zugriff wird die TLS-Verbindung über das Hypertext Transfer Protocol Secure (HTTPS) umgesetzt. Bei einem anderweitigen Zugriff zur Verwaltung (Administration) der Verarbeitungssysteme kommt eine Secure Shell (SSH) in der Version 2 (SSH-2) zum Einsatz. Das gleiche gilt für die Übertragung von Dateien auf solche Systeme (SFTP / FTPS). Die für den Zugriff genutzten Passwörter müssen wenigstens 8 Zeichen (Buchstaben, Zahlen, Sonderzeichen) lang sein und sowohl Groß- als auch Kleinbuchstaben enthalten. Die Passwörter von Timme Hosting werden regelmäßig geändert und dürfen ihrerseits nicht unverschlüsselt vorgehalten werden.

II. Vertraulichkeit

Unbefugten wird der Zugang zu den Systemen, mit denen die Verarbeitung personenbezogener Daten erfolgt, durch eine Zugangskontrolle verwehrt. Die von Timme Hosting betriebenen Server

befinden sich in einem Rechenzentrum in Deutschland sowie bei Bedarf in weiteren Rechenzentren in der Europäischen Union (EU). Die Rechenzentren verfügen über: a) elektronisches Zutrittskontrollsystem mit Protokollierung, b) Hochsicherheitszaun um die gesamte Anlage, c) dokumentierte Schlüsselvergabe an Mitarbeiter und Kunden (jeder Kunde, darunter Timme Hosting, ausschließlich für seine Server-Racks), d) Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude, e) 24/7 personelle Besetzung der Rechenzentren, f) Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen sowie g) Zutritt für betriebsfremde Personen zu den Räumen nur in Begleitung eines Mitarbeiters. Außerdem wird durch eine Zugriffskontrolle gewährleistet, dass ausschließlich die zur Benutzung eines Verarbeitungssystems Berechtigten zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. Dazu wird die Zugangsberechtigung von der Geschäftsleitung vergeben. Mitarbeiter von Timme Hosting werden nur zum Zugang auf die Systeme berechtigt, auf die sie zur Erfüllung ihrer Aufgaben zugreifen müssen. Ist der Zugang auf ein System zur Aufgabenerfüllung nicht mehr erforderlich, wird die Berechtigung wieder entzogen. Der Zugriff erfolgt über verschlüssele Verbindungen mit sicheren Passwörtern. Ebenso eröffnet Timme Hosting den Zugang zu einem Kunden-Server zunächst nur über eine verschlüsselte Verbindung mit einem sicheren Passwort. Das Passwort wird als solches nicht bei Timme Hosting vorgehalten. Der Kunde kann und soll das Passwort ändern und die verschlüsselte Verbindung nutzen. Wählt der Kunde ein unsicheres Passwort oder richtet er eine unverschlüsselte Verbindung ein, liegt dies in seiner Verantwortung. Daten auf den Datei-Servern von Timme Hosting sind vor gegenseitiger Kenntnisnahme geschützt. Zu Test- und Entwicklungszwecken werden von Timme Hosting grundsätzlich nur anonyme Daten genutzt.

III. Integrität

Timme Hosting führt regelmäßige Aktualisierungen (Updates) der genutzten Software, insbesondere Sicherheitsupdates, durch. Außerdem werden Schutzprogramme wie Virenscanner eingesetzt, um die Server vor Schadprogrammen wie Rootkits und Malware zu schützen. Das gleiche gilt für Kunden-Server, soweit dies im vereinbarten Leistungsumfang enthalten ist. Ansonsten liegt es in der Verantwortung des Kunden, regelmäßige Updates durchzuführen und Schutzprogramme einzusetzen. Durch die Verschlüsselung einer Verbindung wird neben der Vertraulichkeit auch die Integrität beim Datentransport sichergestellt. Kunden-Daten werden von Timme Hosting einer eindeutigen Kennung zugewiesen und darüber von Daten anderer Kunde getrennt (logische Trennung). Nutzt der Kunde nach dem Hauptvertrag einen Server allein, sind die darauf befindlichen Daten physisch von den Daten auf anderen Servern getrennt. Durch die Datentrennung wird sichergestellt, dass ein Kunde nicht auf die Daten eines anderen Kunden zugreifen kann. Insbesondere kann ein Kunde mit seinem Systemzugang nicht die Daten eines anderen Kunden zur Kenntnis nehmen, verändern oder löschen. Backups durch Timme Hosting werden ebenfalls auf physisch getrennten Systemen vorgehalten. Die Verantwortung für die Trennung von Daten, die der Kunde auf dem Server selbst verarbeitet, liegt jedoch bei ihm. Bei einer Auftragsverarbeitung wird Timme Hosting (Auftragnehmer) die Daten nur gemäß den Weisungen des Kunden (Auftraggeber) verarbeiten, wobei solche Weisungen dokumentiert werden und die

Dokumentation für die zuständigen Mitarbeiter von Timme Hosting vorgehalten wird. Die Einzelheiten regelt neben dem Hauptvertrag ein gesonderter Vertrag über die Auftragsverarbeitung. Die Server-Daten des Kunden werden nach Vertragsende unwiederbringlich gelöscht, was Timme Hosting dem Kunden auf Verlangen noch einmal gesondert bestätigen wird. Vor einer Entsorgung von Datenträgern werden die darauf befindlichen Daten ebenfalls unwiederbringlich gelöscht (mehrfach überschrieben) oder der Datenträger wird vollständig zerstört (geshreddert). Laufwerke und Anschlüsse für externe Datenträger sind an den Servern grundsätzlich nicht vorhanden oder werden nach der Ersteinrichtung des Servers deaktiviert (BIOS).

IV. Verfügbarkeit

Die Rechenzentren verfügen über eine Netzersatzanlage, die eine unterbrechungsfreie Stromversorgung auch bei Stromausfällen im öffentlichen Versorgungsnetz ermöglicht. Außerdem sind die Serverräume der Rechenzentren klimatisiert, insbesondere um bei höheren Außentemperaturen nachteilige Auswirkungen auf den Betrieb der Server (Überhitzung) zu verhindern. Durch Sicherheitskopien (Backups), die täglich erstellt werden, schützt Timme Hosting die personenbezogenen Daten gegen Zerstörung und Verlust. Die Verfügbarkeit der wesentlichen Server-Funktionen wird laufend überwacht (Monitoring). Fällt eine Funktion aus oder tritt eine Fehlfunktion auf, wird dies sowohl der Geschäftsleitung als auch dem zuständigen Mitarbeiter von Timme Hosting gemeldet. Dies gilt für Kunden-Server jedoch nur, soweit Backups bzw. Monitoring im vereinbarten Leistungsumfang enthalten sind. Ansonsten liegt die Verantwortung dafür beim Kunden. Die Einzelheiten zu einer gewährleisteten Verfügbarkeit regelt der Hauptvertrag.

V. Belastbarkeit

Timme Hosting wählt die Hard- und Software für die eingesetzten Systeme so aus, dass diese nach Art und Umfang der jeweiligen Datenverarbeitung auch mittel- bis langfristig ausreichend ist. Die Auslastung der Systeme wird regelmäßig überprüft und die Hardware erforderlichenfalls erweitert (Upgrade) oder auf ein anderes System mit ausreichender Hard- und Software gewechselt (Migration). Administriert der Kunde den Server nach dem Hauptvertrag selbst oder nutzt der Kunde nach dem Hauptvertrag einen Server mit einer bestimmten Konfiguration / Hardwareausstattung, liegt die Verantwortung für die Überprüfung der Auslastung und ein erforderliches Upgrade / Migration jedoch bei ihm. Vor die Server von Timme Hosting ist eine Firewall geschaltet, die insbesondere Distributed Denial of Service-Angriffe (DDoS) verhindert oder abschwächt. In Systemen, auf denen Timme Hosting selbst personenbezogene Daten verarbeitet, werden grundsätzlich gespiegelte Festplatten (RAID) eingesetzt, so dass der Ausfall einer Festplatte noch nicht zum Ausfall des Gesamtsystems führt. Dies gilt insbesondere für Systeme, auf denen die Daten üblicherweise auch zwischen den regelmäßigen Backups verändert werden. Ob auf einem Kunden-Server RAID eingesetzt wird, hängt dagegen vom vereinbarten Leistungsumfang ab.

VI. Wiederherstellbarkeit

Timme Hosting stellt sicher, dass die eingesetzten Systeme im Störungsfall rasch wiederhergestellt werden können. Durch das Monitoring der Server wird ein solcher Fall grundsätzlich sofort erkannt und gemeldet. Bei schwerwiegenden Störungsfällen, das heißt beim Ausfall einer wesentlichen Funktion oder dem Auftreten einer wesentlichen Fehlfunktion, erreicht die Meldung auch außerhalb der Geschäftszeiten von Timme Hosting den für solche Fälle zuständigen Mitarbeiter (Notdienst). Der Notdienst verfügt über ein Mobiltelefon mit einer speziellen Applikation (App), die ihm eine erste Bewertung von Art und Umfang des Störungsfalls ermöglicht. Zur Wiederherstellung der Funktionsfähigkeit kann der Notdienst den Austausch defekter Hardware veranlassen, die Systemkonfiguration überprüfen und auf das letzte Backup zurückgreifen.

VII. Wirksamkeit

Die beschriebenen Maßnahmen haben sich einerseits bewährt und entsprechen andererseits dem Stand der Technik. Sie werden von Timme Hosting regelmäßig überprüft und erforderlichenfalls aktualisiert. Bei einer Aktualisierung wird jedoch das Schutzniveau der beschriebenen Maßnahmen nicht unterschritten. Wesentliche Änderungen, die sich durch die Aktualisierung ergeben, werden dokumentiert. Außerdem hat Timme Hosting einen Datenschutzbeauftragten benannt, der in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Die Einhaltung der beschriebenen Maßnahmen in den Rechenzentren ist vertraglich sichergestellt und kann jederzeit kontrolliert werden. Ebenso sind die Mitarbeiter von Timme Hosting vertraglich zur Einhaltung des Datenschutzes, insbesondere zur weisungsgemäßen Datenverarbeitung bei einer Auftragsverarbeitung, und zeitlich unbeschränkt zur Vertraulichkeit verpflichtet. Personenbezogene Daten dürfen durch die Mitarbeiter nur auf den geschützten Systemen von Timme Hosting vorgehalten werden. Bei datenschutzrechtlichen Anfragen stehen den Kunden und anderen Personen, die von der Verarbeitung ihrer Daten durch Timme Hosting betroffen sind, sowohl der Datenschutzbeauftragte als auch die Geschäftsleitung von Timme Hosting zur Verfügung. Bei der Installation von Software achtet Timme Hosting auf datenschutzfreundliche Voreinstellungen. Das gleiche gilt für Software, die von Timme Hosting selbst entwickelt und auf den Systemen eingesetzt wird. Insbesondere werden von der voreingestellten Software personenbezogene Daten nur in dem Umfang verarbeitet, wie dies nach dem jeweiligen Zweck der Verarbeitung erforderlich ist.