AUFTRAGSVERARBEITUNGSVEREINBARUNG

zwischen

Gambio GmbH

Parallelweg 30 28219 Bremen vertreten durch den

Geschäftsführer Dr. Felix Hötzinger

– nachfolgend **„Auftragnehmer"**

und dem Kunden

– nachfolgend **„Auftraggeber"** –

– nachfolgend gemeinsam **„Parteien"** genannt – (nachfolgend **„Vertrag"**)

Einzelheiten in Bezug auf die Dienstleistung des Auftragnehmers sind in dem jeweiligen Vertrag zwischen Auftragnehmer und Auftraggeber (nachfolgend **„Hauptvertrag"**) geregelt.

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im geschlossenen Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung 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.

1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1. Der Auftragnehmer ist Anbieter eines Online-Shopsystems. Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Die Details sind in Anhang A aufgeführt.
2. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet die in Anhang A genannten Daten im Auftrag des Auftraggebers zu dem dort genannten Zweck in dem genannten Umfang. Dies umfasst Tätigkeiten, die im Hauptvertrag konkretisiert sind.
2. 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).
3. Die Weisungen werden anfänglich durch den Hauptvertrag 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 Pflichten des Auftragnehmers

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. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
3. Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen werden in Anhang B näher beschrieben. Die 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, 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 Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5. 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.
6. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Dies gilt insbesondere bei unberechtigten oder unbeabsichtigten Zugriffen Dritter auf die Daten sowie bei unberechtigter Weitergabe der Daten an Dritte. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
7. 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. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

9. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Anforderung jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. Die erfolgte Durchführung ist dem Auftraggeber auf Verlangen in Textform zu bestätigen. In besonderen Fällen erfolgt eine Aufbewahrung bzw. Übergabe. Eine Herausgabe von Datensicherungen (Backup) ist nicht geschuldet. Entstehen dem Auftragnehmer Kosten bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber. Der Auftraggeber trägt zudem die Kosten der Aufbewahrung durch den Auftragnehmer, soweit eine solche Pflicht vereinbart wird.
10. Die Übermittlung von Daten in Länder, die nicht Mitglied der Europäischen Union oder Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum sind, findet im Moment nicht statt. Sollte es zu einer Datenübertragung in ein Land kommen, das nicht Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ist, sorgen der Auftraggeber und der Auftragnehmer durch geeignete Maßnahmen für ein angemessenes Datenschutzniveau.
11. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Dies ist der Datenschutzbeauftragte:

    Haye Hösel, externer Datenschutzbeauftragter
    HUBIT Datenschutz
    Anschrift: Lise-Meitner-Str. 2, 28359 Bremen
    Telefon: 0421-33114300
    E-Mail: info@hubit.de

    Über einen Wechsel in der Person des Datenschutzbeauftragten ist der Auftraggeber unverzüglich in Textform zu informieren.
12. 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. Der Auftraggeber hat hierfür die Kosten zu tragen.

4 Pflichten des Auftraggebers

1. Der Auftraggeber ist bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für ihn einschlägigen Datenschutzgesetze verantwortlich.
2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
3. Über die Herausgabe oder Löschung der Daten nach Vertragsende (siehe unter Ziffer 3 Abs. 9) muss der Auftraggeber innerhalb einer vom Auftragnehmer gesetzten Frist entscheiden.
4. Für den Fall, dass eine Datenpanne eintritt und eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DS-GVO, § 15a TMG und/oder § 109a TKG besteht, ist der Auftraggeber für deren Erfüllung verantwortlich.

5 Anfragen Betroffener an den Auftraggeber/Auftragnehmer

1. Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.
2. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wendet, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung in Textform unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

7 Subunternehmer

1. Die Beauftragung von Subunternehmern durch den Auftragnehmer ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen der vorliegenden AV- Vereinbarung erfüllen. Insoweit erteilt der Auftraggeber eine allgemeine Genehmigung. Eine Liste der aktuellen Subunternehmer ist hier abrufbar: https://www.gambio.de/sub.html.
2. Der Auftragnehmer ist verpflichtet, den Auftraggeber über die Absicht zur Beauftragung eines weiteren oder den Austausch eines Subunternehmers durch einen Warnhinweis in dem der laufenden Shop-Administration dienenden Kundenportal und Aktualisierung der eben genannten Übersicht zu informieren. Dies hat jeweils mindestens 14 Tage vor Umsetzung der beabsichtigten Veränderung zu geschehen, um dem Auftraggeber die Möglichkeit zu geben, gegen eine derartige Änderung Einspruch zu erheben. Der Einspruch bedarf eines wichtigen Grundes.
3. Der Auftragnehmer hat Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese die zwischen dem Auftraggeber und dem Auftragnehmer getroffenen Vereinbarungen einhalten können und dies auch tun. Der Auftragnehmer hat insbesondere vorab und während der Vertragsdauer regelmäßig zu kontrollieren, dass Subunternehmer die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben. Das Ergebnis solcher Kontrollen ist vom Auftragnehmer zu dokumentieren

und auf Anfrage dem Auftraggeber zu übermitteln.

4. Sofern der Subunternehmer zur Bestellung eines betrieblichen Datenschutzbeauftragten nach Art. 35ff DS-GVO verpflichtet ist, hat sich der Auftragnehmer diesen benennen zu lassen.
5. Der Auftragnehmer hat durch vertragliche Regelung sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.
6. Der Auftragnehmer hat mit dem Subunternehmer eine Auftragsverarbeitungsvereinbarung zu schließen, die den Voraussetzungen des Art. 28 DS-GVO entspricht.
7. Der Auftragnehmer hat durch vertragliche Regelungen insbesondere sicherzustellen, dass die in diesem Vertrag geregelten Kontrollbefugnisse des Auftraggebers sowie der Aufsichtsbehörden auch gegenüber dem Subunternehmer entsprechend gelten. Es ist ausdrücklich zu vereinbaren, dass der Subunternehmer solche Kontrollmaßnahmen durch den Auftraggeber zu dulden hat.
8. Nicht als Subunternehmer im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

8 Informationspflichten

1. Der Auftraggeber ist unverzüglich in Textform zu informieren, falls eine Datenschutzbehörde den Auftragnehmer bezüglich seines Auftragsverhältnisses mit Auftraggeber kontrolliert, diesbezüglich aufsichtsrechtliche Maßnahmen gegen ihn androht oder verhängt oder aber Ermittlungen wegen diesbezüglicher datenschutzrechtlicher Bußgeld- und Straftatbeständen aufgenommen werden.
2. Unabhängig von etwaigen Datenschutzstörungen, -verletzungen oder -unregelmäßigkeiten bezüglich des Auftragsverhältnisses mit dem Auftraggeber wird der Auftragnehmer dem Auftraggeber auf dessen Anforderung hin einen Bericht über Vorfälle und Vorhaben im Bereich Datenschutz und Datensicherheit mit Bezug zur Auftragserfüllung für den Auftraggeber in Textform übermitteln. Darin soll aufgeführt werden, ob und gegebenenfalls welche Vorfälle es gab sowie etwaige Ergebnisse bzw. Planungen zu internen oder externen Datenschutz Prüfungen.

9 Laufzeit

1. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages. Sollte die Datenverarbeitung über die Laufzeit des Hauptvertrages fortgesetzt werden, bleibt dieser Vertrag so lange in Kraft, bis er von einer Partei mit einer Frist von 3 Kalendermonaten zum Monatsende in Textform gekündigt wird.
2. Können die Parteien im Falle eines Einspruchs gegen den beabsichtigten Einsatz eines neuen bzw. anderen Subunternehmens keine Einigung erzielen, steht beiden Parteien ein Sonderkündigungsrecht zu.

10 Haftung

Die Haftung richtet sich nach dem Hauptvertrag.

11 Sonstiges

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 von Art. 4 Nr. 7 DS-GVO liegt.
2. Änderungen und Ergänzungen dieses Vertrags und aller seiner Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung im Sinne von § 126 Abs. 1 und 2 BGB unter Ausschluss von § 126a BGB 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. Der Auftragnehmer nimmt diesen Vertrag durch einen Vermerk über den Eingang der vom Auftraggeber unterzeichneten Vertragsfassung beim Auftragnehmer in den Kundenstammdaten des Auftraggebers an. Der Auftraggeber verzichtet hiermit auf den Zugang der Erklärung der Annahme seitens des Auftragnehmers gemäß § 151 BGB.
4. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrags den Regelungen des Hauptvertrags vor. Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.
5. Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist Bremen.
6. Anhang A und B sind wesentlicher Bestandteil dieses Vertrags.

Anhang A zur Auftragsverarbeitungsvereinbarung

Bei Nutzung des Gambio Hub:

Gegenstand und Dauer des Auftrags:	Verarbeitung von personenbezogenen Daten zur Bereitstellung des Gambio Hubs auf den Servern von Gambio für die Dauer der Nutzung des Gambio Hubs durch den Auftraggeber.
Art und Zweck der vorgesehenen Verarbeitung von Daten:	Die vom Auftraggeber erhobenen personenbezogenen Daten in seinem Webshop (insbesondere Transaktionsdaten und Stammdaten der Kunden des Auftraggebers (z. B. Name, Anschrift) werden an den Auftragnehmer übertragen und von diesem an die ausgewählten Partnerunternehmen (z.B. Zahlungsdienstleister) weitergeroutet, sofern das für die jeweilige Transaktion erforderlich ist. Die Daten werden auf den Servern von Gambio gespeichert. Der Zweck der Datenverarbeitung ist die Abwicklung von Transaktionen für den Auftraggeber.
Art der personenbezogenen Daten:	Transaktionsdaten und sonstige, für die Nutzung und Bestellung im Webshop des Auftraggebers relevante personenbezogene Daten, insbesondere Personenstammdaten (z. B. Name, Anschrift des Kunden).

Kategorien betroffener Personen:	Kunden und Interessenten des Auftraggebers, die den Webshop des Auftraggebers besuchen und dort den Bestellvorgang durch Eingabe ihrer Daten einleiten.
Löschung, Sperrung und Berichtigung von Daten:	Anfragen zur Löschung, Sperrung und Berichtigung sind an den Auftraggeber zu richten; im Übrigen gelten die Regelungen dieses Vertrages.

Bei Nutzung von Supportleistungen und/oder Beauftragung individueller Entwicklungen oder sonstigen Dienstleistungen (z.B. Installations-Services):

Gegenstand und Dauer des Auftrags:	Beratungs - und Supportdienstleistungen bezüglich der zur Verfügung gestellten Software. Wartung und Anpassung der Software auf Basis individueller Beauftragung durch den Auftraggeber - ggfs. ebenfalls die Sicherung von Daten – nach Maßgabe des jeweiligen Auftrags. Die Dauer richtet sich nach der jeweiligen Vereinbarung mit dem Auftraggeber.
Art und Zweck der vorgesehenen Verarbeitung von Daten:	Die vom Auftraggeber übermittelten personenbezogenen Daten oder Daten, auf die der Auftragnehmer durch Überlassung von Zugangsdaten durch den Auftragsgeber Zugriff erhält. Die Daten können auf den Servern von Gambio gespeichert werden. Der Zweck der Datenverarbeitung ist die Bereitstellung von Beratungs- und Supportdienstleistungen für den Auftraggeber sowie die Wartung, Individualisierung und Konfiguration der Software - ggfs. ebenfalls die Sicherung von Daten – nach Maßgabe des jeweiligen Auftrags.

Art der personenbezogen-en Daten:	Transaktionsdaten und sonstige, für die Nutzung und Bestellung im Webshop des Auftraggebers relevante personenbezogene Daten, insbesondere Personenstammdaten (z. B. Name, Anschrift des Kunden).
Kategorien betroffener Personen:	Kunden und Interessenten des Auftraggebers, die den Webshop des Auftraggebers besuchen, dort ggfs. bestellen und in diesem Zusammenhang ihre personenbezogenen Daten erhoben werden.
Löschung, Sperrung und Berichtigung von Daten:	Anfragen zur Löschung, Sperrung und Berichtigung sind an den Auftraggeber zu richten; im Übrigen gelten die Regelungen dieses Vertrages.

Bei Nutzung der Gambio Cloud:

Gegenstand und Dauer des Auftrags:	Die Bereitstellung eines Onlineshops auf den Servern von Gambio. Die Dauer richtet sich, nach der jeweiligen Vereinbarung mit dem Auftraggeber.
Art und Zweck der vorgesehenen Verarbeitung von Daten:	Sämtliche im Onlineshop bzw. auf dem zur Verfügung gestellten Speicherplatz hinterlegte personenbezogenen Daten, um den zuverlässigen und sicheren Betrieb eines Onlineshops sicherzustellen.
Art der personenbezogen en Daten:	Transaktionsdaten und sonstige, für die Nutzung und Bestellung im Webshop des Auftraggebers relevante personenbezogene Daten, insbesondere Personenstammdaten (z. B. Name, Anschrift des Kunden).
Kategorien betroffener Personen:	Kunden und Interessenten des Auftraggebers, die den Webshop des Auftraggebers besuchen, dort ggfs. bestellen und in diesem Zusammenhang ihre personenbezogenen Daten erhoben werden.
Löschung, Sperrung und Berichtigung von Daten:	Anfragen zur Löschung, Sperrung und Berichtigung sind an den Auftraggeber zu richten; im Übrigen gelten die Regelungen dieses Vertrages.

Anhang B

zur Auftragsverarbeitungsvereinbarung

Technische und organisatorische Maßnahmen (TOM)
Verantwortlicher

Gambio GmbH

Parallelweg 30

28219 Bremen

Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen (TOM) gemäß EU Datenschutz Grundverordnung sind grundlegend für die Datenverarbeitung im Unternehmen. Ergänzende Maßnahmen und / oder Abweichungen sind gegebenenfalls im jeweiligen Verfahren beschrieben.

1 Vertraulichkeit

1.1 Zutrittskontrolle

1.1.1 Gebäude

Das Hauptgebäude bzw. die Büroetage im Nebengebäude werden verschlossen, wenn der letzte Mitarbeiter das Büro verlässt. Im Nebengebäude wird der Eingang zum Treppenhaus ab 18:00 Uhr verschlossen. Es kommen Schließzylinder mit Sicherheitsschloss zum Einsatz.

Mittels Videokameras werden verschiedene Bereiche des Unternehmens außerhalb der Arbeitszeiten überwacht. Die Alarmierung erfolgt per Email, wenn es zu Bildveränderungen kommt.

Die Schlüssel werden durch den Hausmeister gegen Unterschrift auf Weisung der Personalabteilung ausgegeben.

1.1.2 Serverraum

Der Serverraum ist verschlossen. Eine Richtlinie (Dokument: R0006-k230 Schutz von Serverräumen) beschreibt die Zutrittsberechtigten und die Zutrittskontrolle.

1.1.3 Besucher

Besucher werden persönlich in Empfang genommen und dauerhaft beaufsichtigt.

Besucher dürfen sich grundsätzlich nur in den Besucherzonen aufhalten. Besucher, die Arbeitsbereiche betreten, werden dauerhaft begleitet. Weiterhin wird sichergestellt, dass keine personenbezogenen Daten oder schützenswerte Unternehmensdaten einsehbar sind.

1.2 Zugangskontrolle

1.2.1 Papier-Akten

Aktenschränke und das Aktenarchiv sind verschlossen.

1.2.2 Firewall

Das Firmennetzwerk wird nach außen mittels einer Firewall geschützt. Das Intranet wird zusätzlich durch einen Proxy-Server geschützt.

1.2.3 VPN-Zugang

Der VPN-Zugang ist mittels Authentifizierung gesichert und steht nur ausgewählten Personen zur Verfügung.

1.2.4 Datenverarbeitungsanlagen

Jede Datenverarbeitungsanlage (kurz: DVA) wird mittels Authentifizierung geschützt. Zusätzlich kommen software-spezifische Authentifizierungen zum Einsatz. Eine schriftliche *Passwortrichtlinie* (Dokument R0004-k230 Passwortrichtlinie) existiert.

Die manuelle und automatische Sperrung des Arbeitsplatzrechners ist in der *Passwortrichtlinie* (Dokument R0004-k230 Passwortrichtlinie) beschrieben.

1.2.5 Netzwerk-Infrastruktur

Serverschränke sind unter Verschluss.

1.3 Zugriffskontrolle

1.3.1 Datenverarbeitungsanlagen

Aufgrund der Benutzerauthentifizierung werden die Benutzer bestimmten Gruppen zugeordnet. Die Zugriffsfreigabe auf Ordner und Dokumente erfolgt mittels Benutzer- / Gruppenfreigaben. In bestimmten Programmen kommt eine Berechtigungsmatrix zum Einsatz.

1.3.2 WLAN

Das betriebliche WLAN ist verschlüsselt. Der Zugang erfolgt über den jeweiligen Domänenbenutzer.

Für Besucher wird ein ebenfalls verschlüsseltes Gast-WLAN bereitgestellt, welches vom betrieblichen Netzwerk virtuell getrennt ist und nur den Zugang zum Internet ermöglicht. Der Zugang zum Gast-WLAN ist zeitlich beschränkt.

1.4 Fernwartung

Die Fernwartung von Kundensystemen erfolgt über die vom Kunden bereitgestellten Protokolle und Dienste.

Es erfolgt keine Fernwartung durch Fremdfirmen bei dem *Verantwortlichen* .

1.5 Trennungsgebot

Daten, die zu unterschiedlichen Zwecken erhoben, verarbeitet oder genutzt werden, werden getrennt gespeichert.

Die Trennung erfolgt

- innerhalb der eingesetzten Software oder
- durch die Nutzung unterschiedlicher Ordner (-strukturen) oder durch die Ablage in unterschiedlichen Aktenordnern.
- durch logische Trennung (beispielsweise Flags innerhalb einer Datenbank)

Test- und Produktivsysteme sind getrennt.

1.6 Pseudonymisierung / Anonymisierung

Sofern dies möglich oder erforderlich ist, werden Daten pseudonymisiert. Hierbei werden Daten, die einen Personenbezug ermöglichen, entfernt oder durch zufällige Werte überschrieben. Aufgrund eines Schlüssels kann wieder ein Personenbezug hergestellt werden. Der hierfür erforderliche Schlüssel ist nur einem eingeschränkten Personenkreis zugänglich. Angewendete Pseudonymisierungen werden in dem jeweiligen Verfahren beschrieben.
Sofern dies möglich oder erforderlich ist, werden Daten anonymisiert. Hierbei werden Daten, die einen Personenbezug ermöglichen, entfernt oder durch zufällige Werte überschrieben. Es ist nachträglich nicht mehr möglich einen Personenbezug herzustellen. Angewendete Anonymisierungen werden in dem jeweiligen Verfahren beschrieben.

Im Testsystem kommen keine Echtdaten oder anonymisierte Daten zum Einsatz.

2 Integrität

2.1 Weitergabe- / Transportkontrolle

Teilnehmerlisten von Veranstaltungen werden nicht an Aussteller oder Referenten weitergegeben.

Bei der Buchung von Zusatzprodukten bzw. Add-Ons eines Partners erfolgt keine Datenweitergabe an den jeweiligen Partner. Die Buchung des Pakets erfolgt bei dem Partner.

Datenträger in mobilen Notebooks werden verschlüsselt.

Die Datenträger aller Linux-Arbeitsstationen sind verschlüsselt.

Die Weitergabe- bzw. Transportkontrolle ist in dem jeweiligen Verfahren beschrieben.

2.1.1 VPN

VPN-Verbindungen zum Firmennetzwerk sind grundsätzlich verschlüsselt. Nur ausgewählte Mitarbeiter erhalten einen VPN-Zugang.

2.1.2 Datenträgervernichtung

Die Datenträgervernichtung ist in der *Datenschutz-Ordnung* (Dokument: K0001-k230 Datenschutz-Ordnung) geregelt.

2.2 Eingabekontrolle

Die Eingabekontrolle ist in dem jeweiligen Verfahren beschrieben.

3 Verfügbarkeit und Belastbarkeit

3.1 Schutzsoftware

Eine regelmäßig aktualisierte Antivirensoftware schützt alle stationären und mobilen DVA vor Viren, Trojanern, Spyware, Malware und anderer Schadsoftware.

3.2 Datensicherung

Die Datensicherung ist in der *Datensicherungsrichtlinie* (Dokument: R0006-k230 Richtlinie Datensicherung) beschrieben.

Die Datensicherung erfolgt täglich. Die Buchhaltung, Workstation und Anwenderprofile werden in die Datensicherung einbezogen.

Rechenzentrum *Hetzner*:

Die Datensicherung in den externen Rechenzentren erfolgt täglich.

Rechenzentrum *publicompserver*:
Die Datensicherung in den externen Rechenzentren erfolgt täglich.

3.3 Rasche Wiederherstellung des Betriebs

3.3.1 Datenwiederherstellung

Die Festplatten im Server sind als RAID 6 konfiguriert. Das RAID wird gespiegelt.

Aus der Datensicherung können sowohl einzelne Datensätze als auch alle virtuellen und physikalischen Server wiederhergestellt werden.

3.4 Internetanbindung

Es bestehen mehrere Internetanbindungen von unterschiedlichen Providern.

3.5 Stromversorgung

Eine unterbrechungsfreie Stromversorgung (USV) stellt bei Stromausfall die Stromversorgung des Servers für sicher und initiiert ein geordnetes Herunterfahren des Servers. Zudem werden durch die USV Spannungsspitzen abgefangen.

3.6 Monitoring

Serversysteme und bestimmte Netzwerk-Komponenten werden mittels eines automatisierten Monitorings überwacht. Bei Fehlfunktionen und Erreichen von Grenzwerten erfolgt eine Alarmierung der IT.

3.7 Umgebung

In dem Serverraum verlaufen keine Wasserrohre.

4 Datenschutz Management

4.1 Datenschutz-Ordnung / Richtlinien

Es existiert eine *Datenschutz-Ordnung* (Dokument: K0001-k230 Datenschutz-Ordnung), in der grundlegenden Verantwortlichkeiten, Maßnahmen und Erfordernisse beschrieben und geregelt sind. Ergänzend zu der *Datenschutz-Ordnung* existieren Richtlinien, Arbeitsanweisungen und Prozessbeschreibungen. Dies sind beispielsweise:

- Meldung Datenvorfall
- Passwortrichtlinie
- Beteiligung des Datenschutzbeauftragten
- Schutz von Serverräumen
- Verlust von Hardware
- Private Nutzung (Internet, Email, Hardware)
- Einsichtnahme User-Accounts
- Schlüsselordnung
- Clean Desktop

4.2 Datenschutzbeauftragter

Es ist ein Datenschutzbeauftragter bestellt. Die Bestellung eines Datenschutzbeauftragten ist auf der Webseite und durch Aushang veröffentlicht.

Regelmäßig führt der Datenschutzbeauftragte eine Begehung und Audit(s) durch.
Interne Audits werden durch kompetente Mitarbeiter in Absprache mit dem Datenschutzbeauftragten durchgeführt.

4.3 Betroffenenrechte

Für die Wahrung der Rechte der betroffenen Personen (gemäß EU Datenschutz Grundverordnung) existieren Richtlinien und Prozessbeschreibungen.

4.4 Schulung

Die Personen, die mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, werden regelmäßig durch Präsenzschulungen oder Webinare geschult.

4.5 Auftragskontrolle

Die Auftragskontrolle erfolgt durch den *Datenschutzbeauftragten* nach Maßgabe der *Geschäftsführung*.

4.6 Fremde Hard- und Software

Die Verwendung externer bzw. privater Hard- und Software ist in der *Datenschutz-Ordnung* und den dazugehörigen Richtlinien geregelt.