VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

zwischen

der Pflegeeinrichtung
(nachfolgend "**Auftraggeber**" genannt)

und

Ping Pong Labs GbR
Lindenstraße 75
50674 Köln

- Auftragsverarbeiter -
(nachfolgend "**Auftragsverarbeiter**" genannt)

1. Gegenstand und Dauer dieser Vereinbarung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand des Auftrags ergibt sich aus den FAQ der Seite www.recoverapp.de.

(2) Die Dauer dieses Auftrags beginnt mit der Registrierung des Auftraggebers. Diese Vereinbarung endet automatisch und ohne dass es einer Kündigung bedarf mit der rechtlichen Beendigung des Nutzungsverhältnisses des Auftraggebers.

(3) Der Auftraggeber hat das Recht, diesen Vertrag sowie das Nutzungsverhältnis fristlos und ohne das Erfordernis einer vorherigen Abmahnung zu kündigen, wenn der Auftragsverarbeiter gegen die Verpflichtungen nach Ziffern 5, 6 oder 8 oder gegen Weisungen des Auftraggebers verstößt.

2. Konkretisierung des Auftrags

(1) Gegenstand der Auftragsdatenverarbeitung

Der Auftragsverarbeiter stellt dem Pflegeeinrichtung zur Erfüllung der Verpflichtung zur Kontaktnachverfolgung eine technische Lösung zur Verfügung. Die nähere Beschreibung der technischen Lösung ist unter www.recovercare.de zu finden.

(2) Art der personenbezogenen Daten

Gegenstand der Datenverarbeitung durch den Auftragsverarbeiter sind folgende Datenarten/-kategorien:

Persönliche Kontaktdaten

- Vorname
- Nachname
- Telefon
- Adresse
- Check-in/Check-out Zeit
- Name der besuchten Person

(3) Zweck der vorgesehenen Datenverarbeitung

Zweck der Datenverarbeitung ist die Bereitstellung einer technischen Lösung zur Erfüllung der Verpflichtungen für die Pflegeeinrichtung über das Internet. Dadurch wird eine Möglichkeit zur Erfassung der vorgeschriebenen Kontaktdaten für Besucher von

Pflegeeinrichtungen zum Zweck der Nachverfolgung bereitgestellt, die eine Einsichtnahme nur im Bedarfsfall und nur für die Pflegeeinrichtung und die zuständigen Behörden vorsieht.

(4) Kategorien betroffener Personen

Die Datenverarbeitung durch den Auftragsverarbeiter betrifft folgende Personengruppen:

- Besucher der Pflegeeinrichtung
- Bewohner der Pflegeeinrichtung

(5) Ort der Datenverarbeitung

Die Datenverarbeitung durch den Auftragsverarbeiter erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO. Er bestimmt alleine über die Zwecke und Mittel der Datenverarbeitung und ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter, für die Wahrung der Rechte der betroffenen Personen sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

(2) Der Auftraggeber ist berechtigt, dem Auftragsverarbeiter im Rahmen des Auftrags Weisungen zu erteilen. Die Weisungen können insbesondere folgende Aspekte des Auftrags betreffen:

- Festlegung der Verarbeitungsprozesse
- Sicherheitskriterien an das Rechenzentrum
- Einhaltung der Datenschutzbestimmungen

Weisungen erfolgen grundsätzlich schriftlich oder in Textform. In Eilfällen können Weisungen auch mündlich erteilt werden. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform. Weisungsberechtigt ist der Inhaber oder der gesetzliche Vertreter der Pflegeeinrichtung.

4. Rechte und Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Auftrags und nach den dokumentierten Weisungen des Auftraggebers, es sei denn, dass der Auftragsverarbeiter gesetzlich zu einer bestimmten Datenverarbeitung verpflichtet ist. Sofern solche Verpflichtungen bestehen, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, es sei denn, diese Mitteilung ist gesetzlich verboten.

(2) Der Auftragsverarbeiter wird den Auftraggeber unverzüglich in Textform informieren, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(3) Der Auftragsverarbeiter verwendet die zur Datenverarbeitung überlassenen Daten nur im Rahmen dieses Auftrags und nicht für eigene Zwecke oder Zwecke Dritter.

(4) Der Auftragsverarbeiter kennzeichnet Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden. Der Auftragsverarbeiter trennt die personenbezogenen Daten, die er im Rahmen dieses Auftrags für den Auftraggeber verarbeitet, strikt von sonstigen Datenbeständen.

(5) Der Auftragsverarbeiter setzt für die Datenverarbeitung im Rahmen dieses Auftrags nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

5. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die nach Art. 28 Abs. 3 lit. c, 32 DS-GVO in Verbindung mit Art. 5 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen. Dabei handelt es sich um Maßnahmen zur Gewährleistung der Datensicherheit sowie eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.

(2) Der Stand der Technik, die Kosten dieser Maßnahmen für den Auftragsverarbeiter 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 sind hinsichtlich der Reichweite dieser Verpflichtung angemessen zu berücksichtigen. Es ist nach § 64 Abs. 1 BDSG (neu) sicherzustellen, dass bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau gewährleistet ist, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten.

Dabei sind die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(3) Der Auftragsverarbeiter hat die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und diese Dokumentation dem Auftraggeber zur Prüfung zu übergeben. Die vom Auftragsverarbeiter getroffenen und für die Dauer des Auftrags aufrechtzuerhaltenden technischen und organisatorischen Maßnahmen sind in **Anlage A** festgelegt. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(4) Der Auftragsverarbeiter kontrolliert regelmäßig seine internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Datenverarbeitung im Rahmen dieses Auftrags im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(5) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragsverarbeiter berechtigt, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

(6) Soweit eine spätere Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, setzen die Parteien diese Änderungen einvernehmlich um.

6. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragsverarbeiter darf die personenbezogenen Daten, die im Rahmen dieses Auftrags verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

7. Datenschutzbeauftragte

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

8. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Der Auftragsverarbeiter ist auch bei ausgelagerten Nebenleistungen verpflichtet, vertragliche Vereinbarungen mit den jeweiligen Dienstleistern zu treffen sowie geeignete Kontrollmaßnahmen zu ergreifen, um die personenbezogenen Daten des Auftraggebers auch in diesen Fällen angemessen zu schützen und damit Datenschutz und Datensicherheit zu gewährleisten.

(2) Der Auftragsverarbeiter darf geeignete Unterauftragsverarbeiter (also weitere Auftragsverarbeiter) beauftragen.

(3) Erteilt der Auftragsverarbeiter Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragsverarbeiter, dessen datenschutzrechtliche Pflichten aus diesem Vertrag auch dem weiteren Auftragsverarbeiter vertraglich aufzuerlegen.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung nicht in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, so stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen im Sinne von Art. 46 Abs. 2 DS-GVO sicher.

(6) Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Unterauftragsverarbeitern gelten. In dem Vertrag mit dem Unterauftragsverarbeiter sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters und des Unterauftragsverarbeiters deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragsverarbeiter eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragsverarbeitern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen gemäß Ziffer 9 dieser Vereinbarung, auch vor Ort, bei Unterauftragsverarbeitern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Vertrag mit dem Unterauftragsverarbeiter muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO). Der Vertrag mit dem Unterauftragsverarbeiter ist dem Auftraggeber bei entsprechender Nachfrage vorzulegen.

(8) Der Unterauftragsverarbeiter ist Erfüllungsgehilfe des Auftragsverarbeiters. Der Auftragsverarbeiter haftet gegenüber dem Auftraggeber für ein Auswahl- und Überwachungsverschulden. Der Auftragsverarbeiter haftet gegenüber dem Auftraggeber dar-

über hinaus für Pflichtverletzungen des Unterauftragsverarbeiters wie für eigenes Verschulden.

9. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber oder im Einzelfall von ihm zu benennende Prüfer sind zur Überprüfung der Datenverarbeitung durch den Auftragsverarbeiter berechtigt. Entsprechende Kontrollen beim Auftragsverarbeiter haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden dringenden Gründen angezeigt, finden die Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragsverarbeiters statt. Soweit der Auftragsverarbeiter den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten gemäß Ziffer 9.3 dieser Vereinbarung erbringt, beschränken sich die Kontrollen auf Stichproben.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Dies gilt insbesondere auch für die Fälle, in denen der Auftragsverarbeiter die Datenverarbeitung gemäß Ziffer 8 dieser Vereinbarung auf einen Unterauftragsverarbeiter auslagert. Der Auftragsverarbeiter ist dabei verpflichtet, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und Informationen zur Verfügung zu stellen, die zum Nachweis der Einhaltung der Pflichten gem. Art. 28 DS-GVO, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen erforderlich sind.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz);
- die Einhaltung unternehmensinterner Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung;

10. Zusammenarbeit der Parteien gegenüber Behörden und betroffenen Personen

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Art. 30 bis 36 DS-GVO genannten Pflichten. Hierzu gehören insbesondere

- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Eine solche Meldung ist insbesondere in Fällen des Verlusts oder der Veränderung personenbezogener Daten durch ungesicherten Transport von Daten, Abhandenkommen vorn Ordnern und Unterlagen, Verlust oder Diebstahl von EDV-Equipment, Verlust oder Diestahl von Zugangskarten und Passworten/PINs, fehlerhafte Konfiguration von Systemen und Applikationen, nicht ordnungsgemäße Entsorgung oder Lgaerung von personenbezogenen Daten oder eine nicht ausreichende Datensicherheit beim Auftragsverarbeiter erforderlich;

- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

- die Unterstützung des Auftraggebers bei der Erstellung von Verarbeitungsverzeichnissen,

- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung. Dazu wird der Auftragsverarbeiter dem Auftraggeber auf Anfrage unverzüglich sämtliche relevanten Informationen über die vom Auftragsverarbeiter eingesetzten Mittel der Verarbeitung zur Verfügung stellen;

- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Der Auftragsverarbeiter unterstützt den Auftraggeber im Rahmen seiner Informationspflicht gegenüber Betroffenen (Artt. 13, 14 DS-GVO) und stellt ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung.

(3) Der Auftragsverarbeiter unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche der betroffenen Personen bzgl. der in Kapitel III DS-GVO genannten Rechte. Insoweit gewährleistet der Auftragsverarbeiter insbesondere, dass er das Löschkonzept des Auftraggebers und die Geltendmachung des Rechts auf Vergessenwerden, Berichtigung, Einschränkung der Verarbeitung, Datenportabilität und Auskunft sowie einen etwaigen Widerspruch oder Widerruf durch Betroffene nach schriftlicher Weisung des Auftraggebers umsetzen kann.

Die Parteien informieren sich unverzüglich wechselseitig über Anfragen und Ansprüche, die von betroffenen Personen geltend gemacht werden, soweit sie sich auf die-

sen Auftrag beziehen. Dies gilt insbesondere, wenn die betroffenen Personen einen Haftungsanspruch gegen eine oder beide Parteien behaupten.

(4) Der Auftragsverarbeiter unterstützt den Auftraggeber umfassend bei seinen Pflichten nach Artt. 33 und 34 DS-GVO. In diesem Zusammenhang wird er ihm unverzügliche sämtliche verfügbaren Informationen mitteilen, insbesondere eine Beschreibung der Art der Verletzung des Schutzes der personenbezogenen Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze sowie, soweit dies dem Auftragsverarbeiter möglich ist, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten. Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragsverarbeiter nur nach vorheriger Weisung durchführen.

(5) Der Auftraggeber und der Auftragsverarbeiter arbeiten bei Anfragen der Aufsichtsbehörde zur Erfüllung ihrer datenschutzrechtlichen Verpflichtungen zusammen. Die Parteien informieren sich unverzüglich wechselseitig über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt insbesondere, soweit eine zuständige Behörde anlässlich eines Ordnungswidrigkeiten- oder Strafverfahrens in Bezug auf die Datenverarbeitung im Rahmen dieses Auftrags beim Auftragsverarbeiter oder beim Auftraggeber ermittelt.

(6) Auskünfte an Dritte oder betroffene Personen darf der Auftragsverarbeiter nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen leitet der Auftragsverarbeiter unverzüglich an den Auftraggeber weiter.

(7) Die Parteien unterstützen sich wechselseitig nach besten Kräften bei der Verteidigung in einem einschlägigen Ordnungswidrigkeiten- oder Strafverfahren sowie bei der Abwehr von Haftungsansprüchen einer betroffenen Person oder eines Dritten.

(8) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrags enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen. Diese ist in einer gesonderten Vereinbarung zu regeln.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Der Auftragsverarbeiter erstellt keine Kopien oder Duplikate der zur Datenverarbeitung überlassenen Daten ohne Wissen des Auftraggebers. Ausgenommen sind die Anfertigung von Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie die Verarbeitung von Daten, soweit dies im Hinblick auf gesetzliche Aufbewahrungspflichten erforderlich ist.

(2) Der Auftragsverarbeiter händigt dem Auftraggeber jederzeit nach schriftlicher Aufforderung und spätestens bei Beendigung des Nutzungsverhältnisses sämtliche in sei-

nen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse sowie Datenbestände aus, die im Zusammenhang mit diesem Auftrag stehen. Nach Rücksprache mit dem Auftraggeber löscht der Auftragsverarbeiter diese Daten in seinen eigenen EDV-Systemen bzw. vernichtet die entsprechenden Datenträger. Test- und Ausschussmaterial ist ebenfalls datenschutzkonform zu vernichten oder dem Auftraggeber auszuhändigen. Eine Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Auf Wunsch des Auftraggebers bestätigt der Auftragsverarbeiter die ordnungsgemäße Löschung bzw. Vernichtung in Schriftform und mit Datumsangabe.

(3) Der Auftragsverarbeiter stellt eine unverzügliche Rückgabe bzw. Löschung entsprechend Ziffer 11.2 bei eventuellen UnterAuftragsverarbeitern sicher.

(4) Die Einrede des Zurückbehaltungsrechts gem. § 273 BGB ist hinsichtlich der personenbezogenen Daten, die im Rahmen dieses Auftrags verarbeitet werden, und der dazugehörigen Datenträger ausgeschlossen.

(5) Der Auftragsverarbeiter ist berechtigt, Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über die Dauer dieses Auftrags und ggf. die Laufzeit des Hauptvertrags hinaus aufzubewahren.

12. Haftung und Schadensersatz

(1) Nimmt ein Dritter den Auftragsverarbeiter für einen Schaden in Anspruch, für den der Auftraggeber gesamtschuldnerisch mithaftet, insbesondere nach der EU-Datenschutz-Grundverordnung, so wird der Auftraggeber den Auftragsverarbeiter insoweit freistellen, als der Schaden von dem Auftraggeber zu vertreten ist. Der Auftragsverarbeiter stellt den Auftraggeber seinerseits von Ansprüchen Dritter gegen den Auftraggeber frei, die aus einer Verletzung einer Pflicht aus dieser Vereinbarung oder aus einer datenschutzrechtlichen Verpflichtung des Auftragsverarbeiters oder eines vom Auftragsverarbeiters eingesetzten Subunternehmers resultieren.

(2) Der Auftraggeber trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten auch von ihm verarbeitet werden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftraggeber den Auftragsverarbeiter auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragsverarbeiter erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftraggeber dem Auftragsverarbeiter auch sämtliche entstandenen Kosten der Rechtsverteidigung.

13. Schlussbestimmungen

(1) Diese Vereinbarung ist umfassend und abschließend. Nebenabreden wurden nicht getroffen.

(2) Änderungen und Ergänzungen bedürfen der Schriftform. Gleiches gilt für die Abbedingung des Schriftformerfordernisses.

(3) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages hinaus vertraulich zu behandeln.

(4) Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter 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 EU-Datenschutz-Grundverordnung liegen.

(5) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, wird die Gültigkeit dieses Vertrages im Übrigen hiervon nicht berührt. Eine unwirksame Bestimmung gilt als durch eine wirksame Regelung ersetzt, die dem von den Parteien mit der betreffenden Bestimmung verfolgten wirtschaftlichen Zweck in rechtlich zulässiger Weise am nächsten kommt. Dies gilt auch dann, wenn die Unwirksamkeit einer Bestimmung auf einem Maß der Leistung oder der Zeit beruht; es gilt dann das rechtlich zulässige Maß. Entsprechendes gilt für die Füllung etwaiger Lücken in dieser Vereinbarung.

Anlage A

zur

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

Finanzierungsportal der Bürgschaftsbanken

***

TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

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

- **Zutrittskontrolle**

  Maßnahmen die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden verwehren:

  Unbefugten ist der Zutritt zu den Büros, in denen personenbezogenen Daten verarbeitet werden, zu verwehren. Der Zutritt ist ausschließlich für autorisierte Mitarbeiter gestattet. Der Zugang zu dem Bürogebäuden ist mit einem Schließsystem gesichert. Es gibt ein Schlüsselregelung mit dokumentierter Aus- und Rückgabe.

- **Zugangskontrolle**

  Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

  Alle Arbeitsplätze und Dienste sind mindestens über ein Zugangskontrollsystem (Benutzername/Passwort) geschützt.

  Systeme werden, sofern technisch möglich, mit einer Passwortrichtlinie versehen. Aufbau und Lebensdauer der Passwörter sind durch Richtlinien (entsprechend dem IT- Grundschutzkatalog) geregelt.

  Die Daten auf den Rechnern der Mitarbeiter sind vollständig verschlüsselt und nur durch den Nutzer zu entschlüsseln.

  Daten werden nur über ausgewählte Kanäle übermittelt und durch geeignete Maßnahmen verschlüsselt und geschützt. Über nicht verschlüsselte Kanäle werde keine personenbezogenen oder nicht-anonymisierten Daten übertragen.

  Daten in Abhängigkeit des Kanals werden folgendermaßen geschützt:

- Mail: Verschlüsselung des Übertragungswegs (TLS) in Abhängigkeit des Nutzers
- Telefon: Keine Verschlüsselung

- **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 nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

  Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.

  Entwickler im 3rd-Level-Support haben nur Zugriff auf fiktive Testdaten. Mit der Entstörung beauftragtes Personal kann auf reale Daten zugreifen, soweit dies zur Problembehebung notwendig ist. Alle Mitarbeiter haben sich schriftlich zur Einhaltung des Datengeheimnisses verpflichtet.

  In den Büroräumen findet kein Publikumsverkehr statt. Sofern Kunden, Lieferanten oder Handwerker in das Unternehmen kommen, werden sie stets durch einen oder mehrere Mitarbeiter begleitet.

  Die vorgeschriebene Vernichtung von papierhaften Dokumenten mit personenbezogene Daten wird mindestens mit der Sicherheitsstufe P-4 durchgeführt.

- **Trennungskontrolle**

  Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

  Die Daten des Auftraggebers und anderer Mandanten werden soweit möglich von unterschiedlichen Mitarbeitern verarbeitet.

  Es existiert ein dezidiertes Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Mandanten Rechnung trägt.

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

- **Übertragungskontrolle**

  Die Zugriffe auf Server und zentrale Systeme, die vom Unternehmen eingesetzt werden, werden wann immer technisch möglich über verschlüsselte Verbindungen vorgenommen. Für Systeme über die Dritten die Eingabe von Daten ermöglicht wird, wird ebenfalls stets eine Möglichkeit für einen verschlüsselten Zugriff bereitgestellt. Damit wir die Datenintegrität, die Authentizität und die Sicherheit vor fremden Zugriffen gewährleistet. Dazu kommen unter anderem SSH-Tunnel bzw. SSL gesicherte Verbindungen zum Einsatz.

- **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:

Wenn möglich, werden Daten ausschließlich verschlüsselt übertragen (siehe Punkt Zugangskontrolle). Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert bei der verschlüsselten Übertragung (per HTTPS-, SSH-, TLS- oder VPN-Verbindung).

Ein physischer Versand von Datenträgern ist nicht vorgesehen. Dadurch besteht kein Risiko des Verlustes von physischen Datenträgern und es kann zu keinem Missbrauch transportierter Daten kommen.

Daten, welche zur Demonstration des Anliegens oder zum Test der Applikation erforderlich sind, werden vor der Übertragung in das Ticketsystem auf das zur Bearbeitung des Anliegens nötige Mindestmaß reduziert, d.h. die Daten werden soweit möglich anonymisiert oder zumindest pseudonymisiert.

- **Eingabekontrolle**

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

  Es findet eine Protokollierung der Bearbeitung personenbezogener Daten statt. In dieser wird eindeutig zugeordnet und dokumentiert welche personenbezogenen Daten von welchem Bearbeiter geändert, entfernt oder eingegeben wurden.

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

- **Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit**

  Maßnahmen die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

  Alle Arbeitsplätze verfügen über eine Anti-Viren-Software, die automatisch aktualisiert wird und regelmäßige Prüfläufe durchführt.

  Eine inkrementelle Datensicherung (Synchronisation) wird täglich durchgeführt und in unterschiedlichen Brandabschnitten aufbewahrt. Zusätzliche Maßnahmen zur Verfügbarkeitskontrolle sind in den technischen und organisatorischen Maßnahmen der Subunternehmer aufgeführt.

- **Zuverlässigkeit**

  Die eingesetzten Systeme werden regelmäßig getestet, überprüft und aktualisiert. Beim Einsatz externer Systeme wird auf geeignete Garantien für eine regelmäßige Prüfung und Aktualisierung durch den Betreiber geachtet. Fehlermeldungen von Mitarbeitern oder Kunden werden schnellst möglich geprüft, kontrolliert und bei Notwendigkeit korrigiert. Vor der Einführung neuer Systeme, Tools oder Funktionen erfolgen ausgiebige Tests durch mehrere fachkundigen Mitarbeiter.
  Die Backupprozesse werden dokumentiert und die Wiederherstellung einzelner Backups stichprobenartig getestet, um im Falle einer notwendigen Wiederherstellung gewohnte und funktionierende Abläufe zur Hand zu haben. Bei Fehlern im Backup-Prozess werden die zuständigen Mitarbeiter automatisch informiert.

- **Datenintegrität**

  Während die Übertragungskontrolle die Datenintegrität bei der Übertragung sicherstellt und die Speicher- bzw. Datenträgerkontrolle die Integrität der Daten auf den Speichermedien sicherstellt, wird die Integrität von Daten zusätzlich über redundante Backupsysteme sichergestellt, die unabhängig voneinander physikalisch getrennt laufen.

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

- **Datenschutz-Management**

  Der Auftragsverarbeiter hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse. Durch den betrieblichen Datenschutzbeauftragten finden regelmäßige Überprüfungen statt. Diese werden dokumentiert.

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

  - Löschungen in den für die Verarbeitung eingesetzten Systemen können durchgeführt werden (Löschfähigkeit).
  - Es werden nur die gemäß Vorgaben des Auftraggebers erforderlichen Daten verarbeitet.

- **Auftragskontrolle**

  Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

  Die zur Verarbeitung eingereichten Daten werden nur im Rahmen der Weisungen des Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben. Zur Sicherstellung werden unter anderem folgende Maßnahmen umgesetzt:

  - Abschluss einer Vereinbarung zur Auftragsverarbeitung oder von EU- Standardvertragsklauseln
  - Überprüfen von sonstigen Dokumentationen und Rechercheergebnissen, die eine Beurteilung der Zuverlässigkeit eines Subunternehmers ermöglichen
  - Kontrolle der Vertragsausführung

  Die Verarbeitung personenbezogener Daten wird nur entsprechend den Weisungen des Auftraggebers gewährleistet und durch schriftliche Vereinbarungen zum Datenschutz zwischen Auftraggeber und Auftragsverarbeiter festgelegt.