Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

_____ (bitte ausfüllen)
NAME DES UNTERNEHMENS (vollständige Firmierung)

_____ (bitte ausfüllen)
STRASSE HAUSNUMMER

_____ (bitte ausfüllen)
PLZ ORT

(Verantwortlicher - nachstehend *Partner* genannt)

und der

ISB GmbH

Friedenstr. 33

76351 Linkenheim

(Auftragsverarbeiter - nachstehend *Termingo* genannt)

§ 1 Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

1. Der Partner nutzt für sein Unternehmen eine durch Termingo entwickelte Terminierungs-, Terminverwaltungs- und Buchungssoftware („Online-Timer“), mittels er mit seinen Kunden online Termine verbindlich vereinbaren kann.

   Der Online-Timer wird durch Termingo bzw. durch Dienstleister von Termingo gehostet und betrieben sowie technisch und inhaltlich weiterentwickelt und an neue Gegebenheiten angepasst. Termingo erbringt darüber hinaus Leistungen der Systempflege und -Aktualisierung, der Administration sowie den technischen Support hinsichtlich des Online-Timers für den Partner. Ein Zugriff auf die innerhalb des Online-Timer-Systems verarbeiteten personenbezogenen Daten von Kunden des Partners ist im Zuge dieser Tätigkeiten durch Termingo nicht ausgeschlossen.

   Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus diesem Zugriff und der daraus folgenden Auftragsverarbeitung personenbezogener Daten („Daten“) für die Zwecke des Partners ergeben. Diese Vereinbarung umfasst die Erbringung aller Dienstleistungen von Termingo für den Partner in deren Rahmen personenbezogene Daten verarbeitet werden, soweit dies in dieser Vereinbarung dokumentiert ist.

2. Die Verarbeitung von Daten durch Termingo erfolgt nur im vertraglich festgelegten Umfang und für den vorgegebenen Zweck und nach den Weisungen des Partners.

3. Termingo verarbeitet personenbezogene Daten im Auftrag des Partners. Alle Einzelheiten gemäß Art. 28 Abs. 3 Satz 1 DS-GVO (Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie Kreis der betroffenen Personen) sind im ***Anhang, Abschnitte A. - D.*** zu dieser Vereinbarung aufgeführt.

4. Die durch Termingo verarbeiteten personenbezogenen Daten dienen ausschließlich den Zwecken der Vertragserfüllung. Termingo beachtet dabei die einschlägigen datenschutzrechtlichen Bestimmungen. Termingo verpflichtet sich insbesondere, bei der Erbringung seiner Leistungen die Grundsätze der Datenvermeidung und der Datensparsamkeit zu beachten. Eine Verwendung der Daten für andere Zwecke darf nicht erfolgen. Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Partner verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke ist nicht gestattet.

§ 2 Pflichten des Partners

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist der Partner verantwortlich. Das alleinige Verfügungsrecht über die Daten verbleibt beim Partner.

2. Der Partner hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der bei Termingo getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

3. Der Partner informiert Termingo unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung des Ergebnisses der Auftragsleistung feststellt.

§ 3 Technisch-organisatorische Maßnahmen

1. Termingo hat die Sicherheit der Verarbeitung gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO zu gewährleisten und auf Dauer herzustellen. Insgesamt handelt es sich bei den von Termingo zu treffenden technischen und organisatorischen Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten sind im ***Anhang, Abschnitt G.*** dokumentiert].

2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es Termingo gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3. Termingo gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 Buchst. d DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

1. Termingo darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Partners berichtigen, löschen oder deren Verarbeitung einschränken.

2. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an Termingo, wird Termingo die betroffene Person an den Partner verweisen, sofern eine Zuordnung an den Partner nach Angaben der betroffenen Person möglich ist. Termingo leitet den Antrag der betroffenen Person unverzüglich an den Partner weiter. Termingo unterstützt den Partner im Rahmen seiner Möglichkeiten auf Weisung.

§ 5 Qualitätssicherung und sonstige Pflichten von Termingo

Termingo hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Termingo setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und soweit relevant auf das Telekommunikationsgeheimnis nach § 3 Telekommunikation-Telemedien-Datenschutzgesetze (TTDSG) verpflichtet und in geeigneter Weise mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Termingo und jede Termingo unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Partners verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Termingo muss durch entsprechende (technisch-organisatorische) Maßnahmen jederzeit sicherstellen, dass kein Zugriff auf die Daten durch Unbefugte erfolgen kann.

b) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten im ***Anhang, Abschnitt G.*** zu dieser Vereinbarung].

c) Der Partner und Termingo arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Die unverzügliche Information des Partners über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei Termingo ermittelt.

e) Soweit der Partner seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei Termingo ausgesetzt ist, hat ihn Termingo nach besten Kräften zu unterstützen.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Partner im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

g) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

h) Daten des Partners dürfen nicht im öffentlichen Raum (z. B. Flughafen, Bahn etc.) verarbeitet werden. Die Verarbeitung der Daten des Partners außerhalb der Geschäftsräume von Termingo ist nur im nichtöffentlichen Raum zulässig und nur mit gesicherten firmeneigenen Geräten von Termingo, welche mit angemessenen technischen und organisatorischen Schutzmaßnahmen nach dem Datensicherheitskonzept von Termingo entsprechend des ***Anhangs, Abschnitt G.*** zu dieser Vereinbarung abgesichert sind.

i) Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Partners nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrages erforderlich ist. Sie sind nach Abschluss der Verarbeitung oder Nutzung vom Termingo unverzüglich datenschutzgerecht zu löschen oder zu vernichten oder dem Partner auszuhändigen. Hiervon ausgenommen sind Sicherheitskopien und sonstige Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Durchführung des Auftrages erforderlich sind, sowie Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen.

§ 6 Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die Termingo z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Termingo ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Partners auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2. Die Beauftragung von Unterauftragnehmern ist nur zulässig, wenn Termingo die nachfolgenden Bestimmungen beachtet. Soweit der Abschluss etwaiger Unterauftragsverhältnisse, die im Zusammenhang mit der für den Partner erbrachten Dienstleistung stehen erfolgt, verpflichtet sich Termingo, den Partner über den Abschluss vorab zu informieren. Bei Vertragsschluss bestehende Unterauftragsverhältnisse werden durch Termingo im ***Anhang, Abschnitt E.*** aufgelistet.

3. Soweit eine Auslagerung auf den Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers nach Abs. 2 erfolgt, ist die Beauftragung von Unterauftragnehmern nur zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird und damit die in der vorliegenden Datenschutzvereinbarung getroffenen Regelungen auch gegenüber Unterauftragnehmern gelten.

4. Termingo hat den Partner über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern zu informieren, so dass der Partner die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DS-GVO). Die Information durch Termingo, die die maßgeblichen Informationen zum Unterauftragnehmer und dessen Auswahl enthalten muss, kann per Textform (E-Mail) erfolgen. Die E-Mail ist zu richten an den oder die im ***Anhang, Abschnitt F.*** genannten Ansprechpartner des Verantwortlichen.

   Erfolgt innerhalb einer Frist von 20 Arbeitstagen keine Rückmeldung per Textform seitens des Verantwortlichen, gilt ein Einspruch als nicht erteilt. Auch für den Einspruch ist Textform (E-Mail) ausreichend. Der Einspruch ist zu richten an den in Anhang 4 definierten Ansprechpartner von Termingo.

5. Termingo ist verpflichtet, vor Beginn der Datenverarbeitung durch den Unterauftragnehmer und sodann in regelmäßigen Abständen die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen - insbesondere der vom Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen - im erforderlichen Umfang zu kontrollieren. Die Weitergabe von personenbezogenen Daten des Partners an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

§ 7 Kontrollrechte des Partners

1. Der Partner hat das Recht, im Benehmen mit Termingo Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch Termingo in dessen Geschäftsbetrieb zu überzeugen.

2. Termingo stellt sicher, dass sich der Partner von der Einhaltung der Pflichten von Termingo nach Art. 28 DS-GVO überzeugen kann. Termingo verpflichtet sich, dem Partner auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

3. Der Partner, dessen Aufsichtsbehörde, die zuständigen Datenschutzbehörden, beauftragte Mitarbeiter und sonstige Beauftragte des Partners (z.B. Prüfdienstleister) sind befugt, Auskünfte bei Termingo einzuholen, die Umsetzung der technischen und organisatorischen Maßnahmen vor Ort während der üblichen Geschäftszeiten von Termingo bei Termingo zu überprüfen und dazu auch die prüfungsrelevanten Örtlichkeiten zu betreten und Einsicht in die erforderlichen Unterlagen und Systeme/Programme - welche den Partner betreffen - zu nehmen. Termingo stellt dabei sicher, dass sich der Partner von der Einhaltung der Pflichten von Termingo nach Art. 28 DS-GVO und der vertraglichen Vereinbarung überzeugen kann.

4. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch 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).

§ 8 Verhalten bei Datenschutzverstößen

Termingo unterstützt den Partner bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Partner zu melden;

b) die Verpflichtung, dem Partner im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

c) die Unterstützung des Partners im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde;

d) Meldung von Störungen des Verarbeitungsablaufs;

e) die Meldung bei Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde;

f) die Meldung bei Ermittlungen durch zuständige Behörden nach Art. 83 und/oder 84 DS-GVO.

§ 9 Weisungsbefugnis des Partners

1. Der Partner behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein jederzeitiges, umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

2. Mündliche Weisungen bestätigt der Partner unverzüglich (mind. Textform).

3. Termingo hat den Partner unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Termingo ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Partner bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

1. Nach Abschluss der vertraglichen Arbeiten hat Termingo sämtliche in seinen Besitz gelangten Daten, Datenträger und Unterlagen sowie Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit der Erfüllung der Leistung stehen, dem Partner auszuhändigen bzw. zu übermitteln. Termingo verwendet die zur Datenverarbeitung überlassenen Daten nicht anderweitig und bewahrt sie nicht länger auf, als es zur Vertragserfüllung erforderlich ist und es der Partner unter Berücksichtigung der Aufbewahrungspflichten bestimmt. Nach Erledigung des Auftrages sind die bei ihm gespeicherten Daten nicht reproduzierbar zu löschen bzw. datenschutzgerecht physisch zu vernichten. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch Termingo entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Termingo kann sie zu seiner Entlastung bei Vertragsende dem Partner übergeben.

2. Die bei der Verarbeitung ggf. entstandenen Arbeitsdateien, die personenbezogene Daten enthalten, sind unmittelbar nach Beendigung/nach dem Versand zu löschen. Ebenso sind alle elektronischen Dateien und Datenbanken sowie Datenträger nicht reproduzierbar zu löschen bzw. datenschutzgerecht physisch zu vernichten. Dies gilt auch für erzeugte Test- und Zwischenergebnisse und Ausschussmaterial.

3. Test- und Ausschussmaterial wird durch Termingo der sofortigen datenschutzgerechten Entsorgung und Vernichtung zugeführt.

4. Die Löschung der personenbezogenen Daten hat nach der DIN-Norm 66399 zu erfolgen und ist mit geeigneten Maßnahmen zu protokollieren. Personenbezogene Daten und/oder Betriebs- und Geschäftsgeheimnisse des Partners sind mindestens auf Schutzklasse 2 und Sicherheitsstufe 4 zu vernichten. Termingo wird vertraglich sicherstellen, dass die Vorgabe des Partners zu DIN-Norm 66399 auch gegenüber Unterauftragnehmern gelten.

5. Termingo schließt durch geeignete Maßnahmen eine unbefugte Duplizierung der auftragsgemäß verarbeiteten Datenbestände aus. Die bei der Verarbeitung ggf. entstandenen Arbeitsdateien, die personenbezogene Daten enthalten, sind unmittelbar nach Beendigung der Produktion /nach dem Versand zu löschen. Die Datenträger werden nach Erfüllung des Auftrages zurückgegeben. Bei einem eventuell erforderlichen Hardware- und/oder Softwareaustausch hat Termingo dafür zu sorgen, dass keine Daten des Partners an Dritte weitergegeben werden, insbesondere, dass Datenspeicher vor der Weitergabe an Dritte datenschutzkonform (nichtreproduzierbar bzw. physisch) vernichtet werden.

§ 11 - Besondere Sicherheitsbedingungen

1. Folgende Klauseln gelten nur dann und insoweit, falls im Rahmen der Auftragsverarbeitung

   - der Zutritt von Termingo in den Räumen des Partners erforderlich ist,
   - eigene Systeme der Partnerin genutzt werden oder
   - Zugriffe auf das interne Netz der Partnerin von außen stattfinden (z.B. Fernwartung).

2. Termingo unterliegt in den Gebäude- und Grundstücksbereichen des Partners den Kontrolleinrichtungen (Zutritts-, Zugangs- und Zugriffskontrolle) sowie den Verhaltensgrundsätzen und –Richtlinien des Partners.

3. Für die Dauer der notwendigen Maßnahmen wird durch den Partner ggf. ein verschlüsselter/zugriffsgeschützter Verbindungsaufbau frei geschaltet.

4. Termingo ist es nicht gestattet, EDV-Geräte, die nicht vom Partner zur Verfügung gestellt werden, ohne vorherige Genehmigung des Partners an das interne Netz bzw. die Telekommunikationseinrichtungen des Partners anzuschließen

§ 12 Haftung

1. Termingo haftet dem Partner gegenüber für sämtliche finanzielle Schäden des Partners auf Grund eines schuldhaften Verstoßes gegen eine Pflicht aus Gesetz (insb. DS-GVO, BDSG) oder aus dieser Vereinbarung. Hiervon sind diejenigen Schäden und Aufwendungen umfasst, die dem Partner aufgrund behördlicher Sanktionen aus einem Verstoß gegen die DS-GVO entstehen (einschließlich der Rechtsverteidigungskosten in Höhe der erstattungsfähigen gesetzlichen Gebühren, vorausgesetzt, dass der Partner Termingo vollumfänglich über die geplanten Maßnahmen der Rechtsverteidigung informiert und diese jeweils mit ihm vorher abstimmt. Termingo haftet nicht, soweit Termingo nachweist, dass Termingo für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist. Im Übrigen gelten im Rahmen dieses Vertrages die Haftungsbestimmungen des dieser Vereinbarung zugrundliegenden Hauptvertrages.

2. Betroffene, welche durch die Übermittlung ihrer Daten an Termingo oder die Verarbeitung durch diesen einen Schaden erleiden, sind berechtigt, wahlweise von Termingo als auch vom Partner Schadenersatz zu verlangen. Die Parteien haften insoweit gesamtschuldnerisch und können nur von der Haftung befreit werden, wenn sie nachweisen, dass keiner von ihnen für den erlittenen Schaden verantwortlich ist. Vorrangig tritt gegenüber den Betroffenen der Partner für den Ersatz des Schadens ein. Für die interne Ausgleichspflicht dieser Gesamtschuldnerschaft gilt § 426 BGB nach Maßgabe der vorstehenden Bestimmungen.

§ 13 Geheimhaltung

Die Vertragsparteien verpflichten sich, sämtliche Informationen und Daten, die Ihnen aus dem Geschäftsbereich des jeweils anderen Vertragspartners bekannt werden, vertraulich zu behandeln und als Geschäftsgeheimnis des anderen Vertragspartners zu wahren. Die Geheimhaltungspflicht besteht auch über das Ende des Vertragsverhältnisses hinaus.

§ 14 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

§ 15 Wirksamkeit des Vertrages und Gerichtsstand

1. Diese Vereinbarung wird Bestandteil des zwischen dem Partner und Termingo geschlossenen Vertrags hinsichtlich der Nutzung des Online-Timers und tritt gemäß Ziffer 8.2. der Allgemeinen Geschäftsbedingungen der ISB GmbH (AGB) durch den Eingang der durch den Partner gegengezeichneten Vertragsdokuments (mindestens in Textform) in Kraft.

2. Alle Änderungen und Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit wenigstens der Schriftform. Das gilt auch für die Änderung des Schriftformerfordernisses selbst.

3. Wesentlicher Vertragsbestandteil dieser Vereinbarung sind die **Anhänge** sowie alle während ihrer Laufzeit abgeschlossenen, weiteren ***Anhänge und Zusatzvereinbarungen***, die ebenfalls der Textform bedürfen.

4. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

5. Der Gerichtsstand für sämtliche Streitigkeiten aus dieser Vereinbarung ist der Sitz von Termingo.

_____ , den _____
Ort Datum
(bitte ausfüllen)

_____ _____

Unterschrift Partner

Unterschrift Termingo

Sarah Thorwart (Geschäftsführung)

_____
Name, Funktion im Betrieb des Partners
(bitte ausfüllen)

Anhang zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

A. Dauer und Laufzeit des Auftrags

Die Dauer dieses Vertrages richtet sich nach der Laufzeit des zwischen den Parteien geschlossenen Kooperationsvertrags Online Timer, inklusive etwaiger Zusatz- und Anschlussvereinbarungen – nachstehend „Hauptvertrag“ genannt. Sie erlischt, wenn der Hauptvertrag, zu dem diese Datenschutzvereinbarung geschlossen wurde, ausläuft oder gekündigt wird und die Verarbeitung personenbezogener Daten durch Termingo zu Zwecken des Vertrags beendet ist.

B. Gegenstand des Auftrags, Umfang, Art und Zweck der Datenverarbeitung

Der Online-Timer (eine Terminierungs-, Terminverwaltungs- und Buchungssoftware) ermöglicht es dem Partner online über ein Webportal mit seinen Kunden Terminbuchungen vorzunehmen. Hierzu besteht ein Kundenprofil auf dem Webportal, in welches durch den Partner selbst auf das eigene Leistungsangebot und auf seine Mitarbeiter etc. angepasst wird. Die Verwaltung des Online-Timers ist für den Partner nach Einloggen in den Kundenbereich online zugänglich und er ist hier in der Lage seine Termine vor Ort zu verwalten und diese im Terminmanagementsystem einzubinden, so dass er jederzeit den Terminverlauf aktualisiert online einsehen kann. Der Partner kann Details und Informationen zur Darstellung seines Profils anlegen sowie die für Terminbuchungen auf der Website notwendigen Angaben und sein Leistungsangebot einpflegen.

Nach den zwischen den Parteien geschlossenen Vereinbarungen wird der Online-Timer durch Termingo technisch und inhaltlich weiterentwickelt und an neue Gegebenheiten angepasst und Termingo erbringt darüber hinaus Leistungen der Systempflege, -Administration und -Aktualisierung sowie den technischen Support hinsichtlich des Online-Timers für den Partner.

C. Kreis der betroffenen Personen

Der Kreis der Betroffenen besteht aus folgenden Personengruppen:

- Geschäftskunden des Partners
- Mitarbeiter und Auszubildende des Unternehmens
- Endkunden (Verbraucher) des Unternehmens
- Interessenten des Unternehmens
- Sonstige Kontaktpersonen

D. Kategorien personenbezogener Daten

Die Kategorien der personenbezogenen Daten sind die Folgenden:

- Namen,
- Adressdaten,
- Kontaktdaten (Email, Mobilfunkrufnummer),
- Vertragsdaten,
- Leistungs- und Angebotsdaten,
- Gesprächshistorie,

- Angaben zur beruflichen Tätigkeit, Qualifikationsdaten
- **Sonstige**: Angaben und Details zur Durchführung und Leistungen der Terminbuchungen in des Unternehmen;
- **Besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO**: In Einzelfällen ggfs. Gesundheitsdaten oder Daten zur ethnischen Herkunft, soweit diese Gegenstand der Online-Korrespondenz zwischen des Unternehmen und deren Endkunden sind.

E. Durch Termingo beauftragte Unternehmen gemäß § 6 Abs. 2 des Vertrags zur Auftragsverarbeitung

	Zweck der Unterbeauftragung/ Gegenstand der Leistungen	**Name und Anschrift des Unternehmens/der verantwortlichen Stelle (ggfs. Ansprechpartner Datenschutz)**	**Ggfs. Anmerkungen**
	Bereitstellung von Online-Speicher und Serverhosting-Dienstleistungen	**netzhaut GmbH** Friedrich-Bergius-Ring 12 97076 Würzburg	Vertrag zur Auftragsverarbeitung liegt vor.
	Versand von Terminbestätigungen per SMS; Esendex ist Dienstleister für den Versand von terminbezogenen SMS Nachrichten an die Terminbucher.	**Esendex** Commify Germany GmbH Radeberger Str. 1 01099 Dresden	Vertrag zur Auftragsverarbeitung liegt vor.
	Versand von Terminbestätigungen per E-Mail; Sendinblue ist Dienstleister für den Versand von terminbezogenen Email Nachrichten an die Terminbucher und Filialinhaber.	**Sendinblue GmbH** Köpenicker Straße 126 10179 Berlin Telefon: +49 (0)30 / 311 995 10	Vertrag zur Auftragsverarbeitung liegt vor.

F.

F.

F. Wechselseitige Ansprechpartner

(1) Autorisierte Kontaktperson(en) des Partners:

Als interne(r) Ansprechpartner und Projektleiter stehen die folgenden Personen im Betrieb der Partnerin zur Verfügung. Die benannten Personen sind zugleich zur Erteilung von Weisungen nach § 9 dieses Vertrags gegenüber Termingo berechtigt:

_____
(Name, Vorname, Funktion/Abteilung, Telefon, E-Mail – bitte ausfüllen)

_____
(Name, Vorname, Funktion/Abteilung, Telefon, E-Mail – bitte ausfüllen)

_____
(Name, Vorname, Funktion/Abteilung, Telefon, E-Mail – bitte ausfüllen)

(2) Autorisierte Kontaktperson(en) von Termingo:

Als autorisierte Ansprechpartner von Termingo und zur Empfangnahme von Weisungen i.S.d. § 9 dieser Vereinbarung sind die folgende(n) Personen berufen:

- *Sarah Thorwart, Geschäftsführer, ISB GmbH, ISB GmbH, Friedenstr. 33, 76351 Linkenheim, sarah.thorwart@isb-software.de, 07247 / 946090*

- *Simon Thorwart,* Geschäftsführer, ISB GmbH, ISB GmbH, Friedenstr. 33, 76351 Linkenheim, simon.thorwart@isb-software.de, 07247 / 946090

G. Dokumentation der von Termingo nach 32 DS-GVO zu treffenden technischen und organisatorischen Maßnahmen

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Alarmanlage - Einsatz einer Alarmanlage (evtl. mit Meldung an Sicherheitsdienst)
- Besucherprotokollierung - Protokollierung der Besucher (z. B. Besucherbuch)
- Bewegungsmelder - Bewegungsmelder
- Chipkarten - Chipkarten-/Transponder-Schließsystem
- Empfang - Besucherkontrolle am Empfang
- Manuelles Schließsystem - Manuelles Schließsystem mit Schließzylinder
- Pförtner - Personenkontrolle beim Pförtner
- Schließanlage - Einsatz einer Schließanlage
- Videoüberwachung - Videoüberwachung der Zugänge

Externe Rechenzentren der Server:

- Festgelegte Sicherheitsbereiche
- Individuelle Zutrittsberechtigungsvergabe
- Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen
- Dokumentationen von Zutrittsberechtigungen
- Zutrittsdokumentation
- Autorisiertes Wachpersonal 24/7
- Sichtkontrollen
- Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)
- Besucher-Regulierungen
- Regelmäßige Kontrollgänge durch das Sicherheitspersonal außerhalb des RZ-Bereiches
- Automatisches Zuziehen und Verschließen von Türen
- Schließung aller Gebäudeeingänge, wie Fenster und Türen
- Zusätzliche mechanische Schutzmaßnahmen für das Erdgeschoss
- Büroräume außerhalb der Arbeitszeit sind verschlossen
- Schutz und Beschränkung der Zutrittswege

- Transponder- oder schlüsselkartenbasierte Schließanlage
- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes
- Alarmmeldungen können von vor Ort befindlichem Personal eingesehen werden
- Eingezäuntes Gelände inkl. Videoüberwachung
- Zutrittskontrollsystem mit Zutrittskarten
- Zusätzliche Zugangsbeschränkung der Serverräume

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort - Authentifikation mit Benutzer + Passwort
- Benutzerberechtigungen - Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt)
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal
- Sperren von externen Schnittstellen - Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren
- Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten
- Protokollierung von Benutzer relevanten Aktivitäten (Anmeldung, Abmeldung,
- Zugangsverweigerungen, etc.)
- VPN-Beschränkungen
- W-LAN-Verschlüsselung (WPA2)
- Regelmäßige Software-Updates
- Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich
- Einschränkung der zeitlichen Gültigkeit der Benutzerkonten
- Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins
- Zwangs- oder Pflicht-Änderung der Kennwörter nach der ersten Anmeldung
- Erforderliche Mindestkomplexität für Kennwörter
- Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes

- Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder
- vergessenen Authentifizierungsdatensatzes
- Verschlüsselte Speicherung von User-Passwörtern
- Zweifaktor Authentifizierung
- User-Login-Verlauf

M.1.3 Beschreibung der Zugriffskontrolle:

- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern - Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren
- Verschlüsselung von Smartphones - Verschlüsselung von Smartphones mit dem Stand der Technik entsprechenden Verfahren

Externe Rechenzentren der Server:

- Vernichtung von physikalischen Medien nach DIN 66399
- Nutzung eines Aktenvernichters (gem. DIN 66399)

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit S/MIME oder PGP Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren)
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig)
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem

M.1.6 Beschreibung der Pseudonymisierung:

- Kennziffern - Verwendung von Kennziffern für Kunden, Patienten oder Personal anstatt Namen
- Trennung Stammdaten - Trennung von Kundenstammdaten und Auftragsdaten

M.1.7 Beschreibung der Verschlüsselung:

- Speicherung - Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard)
- Übertragung - Verschlüsselte Datenübertragung (z.B. E-Mailverschlüsselung nach PGP oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL, Einsatz FTAPI - Datentransfertool)

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

Externe Rechenzentren der Server:

- Rollenbasiertes Berechtigungskonzept (Lesen / Schreiben / Ändern / Kopieren / Löschen)
- Dokumentation der Vergabe von Zugriffsrechten
- Strenge administrative Aufgabentrennung
- Protokollierung von externen Support-Prozessen
- Dokumentation der Weitergabe von physischen Speichermedien
- Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage
- Separate Instanzen für Entwicklungs- und Produktivsysteme (Sandboxes)
- Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff /
- Berechtigungskonzept

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Backup- und Recoverykonzept - Erstellen eines Backup- und Recoverykonzepts

- Brandmeldeanlagen - Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte - CO2 Feuerlöschgeräte in Serverräumen
- IT-Notfallplan - Erstellung und Anwendung von IT-Notfallplänen
- Klimaanlage - Klimaanlage in Serverräumen
- Redundante Datenhaltung - Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum)
- Schutzsteckdosenleisten - Schutzsteckdosenleisten in Serverräumen
- Temperaturüberwachung - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Unterbrechungsfreie Stromversorgung - (USV) Unterbrechungsfreie Stromversorgung

Externe Rechenzentren der Server:

- Schutz der Infrastruktur durch Hardware-Firewalls
- Software-Firewall
- Antivirus-Software
- Überwachung und Protokollierung von administrativen Systemzugang und von
- Konfigurationsänderungen
- Kontrollierter Zugang zu E-Mails und Internet
- Trennung von Anwendungs- und Administrationszugängen
- Überwachung und Protokollierung allgemeiner Benutzeraktivität
- Protokollierung von externen Support-Prozessen
- Protokollierung von administrativen Änderungen
- Zugriffsregelungen und Zugriffsverwaltung
- Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
- Unterbrechungsfreie-Stromversorgung (USV)
- Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr bzw. bei lokalem Sicherheitspersonal
- Kühlsystem im Rechenzentrum / Serverraum
- Automatische Brandlöschanlage
- Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich
- Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern
- Notfallplan

- Externe Audits und Sicherheitstests
- Klar definierte Verwaltungsaufgaben für Partner und Termingo

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen
- Notfallpläne - IT-Notfallpläne und Wiederanlaufpläne

Externe Rechenzentren der Server:

- Disaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
- Tägliche inkrementelle Datensicherung
- Wöchentliche vollständige Datensicherung
- Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
- Auswahl - Auswahl von Termingo unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- Laufende Überprüfung - Laufende Überprüfung von Termingo und seiner Tätigkeiten
- sorgfältige Auswahl Termingo
- regelmäßige Kontrolle der Dienstleister
- gesetzeskonforme AV-Verträge

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Audits - Durchführung regelmäßiger interner Audits
- DSB - Benennung eines Datenschutzbeauftragten
- Managementsystem Datenschutz - Managementsystem zum Datenschutz („DSB360“)
- Managementsystem Informationssicherheit - Managementsystem zur Informationssicherheit (z.B. in Anlehnung an ISO 27001 oder VdS 3473)

- Schwachstellenanalysen - Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest)
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. audatis MANAGER)
- Es existiert ein Datenschutzmanagementsystem mit festgelegten Verantwortlichkeiten, Richtlinien und Abläufen, welches vom Datenschutzbeauftragten und dem Datenschutzteam regelmäßig überprüft wird.