Vertrag
über die Verarbeitung personenbezogener Daten

- nachfolgend „Vertrag“ genannt -

zwischen

Kundennummer: _____

Firma: _____ / HR _____

Ansprechpartner: _____

Straße: _____

PLZ + Ort _____

Land _____

- nachfolgend „**Auftraggeber**“ oder „Verantwortlicher“-
und
LiWiNeA GmbH HRB 12257
vertreten durch den Geschäftsführer: Jan Schumacher
Zum Haunert 22
DE-59519 Möhnesee

- nachfolgend „**Auftragnehmer**“ oder „Auftragsverarbeiter“ -

einzeln oder gemeinsam auch „**Partei**“ und/oder „**Parteien**“

ÄNDERUNGEN AN DIESEM DOKUMENT ZUR ZUM DOWNLOAD BEREITGESTELLTEN VERSION NICHT NICHT ERLAUBT UND GELTEN ALS NICHT GESCHRIEBEN. BITTE KREUZEN SIE NICHTS AN UND ERGÄNZEN SIE DIESEN VERTRAG LEDIGLICH AUF SEITE 1, SEITE 10 UND SEITE 12 UM IHRE ANGABEN. SENDEN SIE DIESEN VERTRAG DANN BITTE ALS PDF DATEI-SCAN AN DATENSCHUTZ@SIMPLYROOT.DE ODER PER POST AN DIE O.G. ADRESSE.

INHALTSVERZEICHNIS

PRÄAMBEL

1 BEGRIFFSBESTIMMUNGEN

Im Sinne dieses Vertrages bezeichnet der Ausdruck

(a) „**Auftragsverarbeiter**“: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet; Auftragsverarbeiter“ ist die im Vorstehenden als „Auftragsverarbeiter“ bezeichnete Vertragspartei.

(b) „**Dritter**“: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

(c) „**Hauptvertrag**“ den in § 2 näher gekennzeichneten Dienstleistungs- oder Kooperationsvertrag.

(d) „**Verantwortlicher**“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

„Verantwortlicher“ ist die im Vorstehenden als „Verantwortlichen“ bezeichnete Vertragspartei, die hier in diesem Vertrag allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(e) „**Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

(f) „**personenbezogene Daten**“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(g) „**weiterer Auftragsverarbeiter oder Unterauftragsverarbeiter**“ den Vertragspartner des Auftragsverarbeiters, der von diesem mit der Durchführung bestimmter Verarbeitungsaktivitäten für den Verantwortlichen beauftragt wird;

(h) „**Sub-Unterauftragsverarbeiter**" den Vereinbarungspartner des weiteren Auftragsverarbeiters oder Unterauftragsverarbeiters, der von Letzterem mit der Durchführung bestimmter Verarbeitungsaktivitäten im Regelungsbereich dieses Vertrags beauftragt wird.

2 GEGENSTAND DES VERTRAGS, RECHTSGRUNDLAGE

(1) Die Rechtsgrundlagen dieser Vereinbarung liegen den Bestimmungen der EU-Datenschutzgrundverordnung (DS-GVO) ab deren Geltungsdatum zugrunde.

(2) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten (nachstehend „Daten" genannt) durch den Auftragsverarbeiter für den Verantwortlichen in dessen Auftrag und nach dessen Weisung im Zusammenhang mit Internet Dienstleistungen auch in Ergänzung des bestehenden Vertrags der Parteien, (nachstehend „Hauptvertrag" genannt) oder einem Neuvertrag.

(3) Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen in Verbindung mit **Annex 1**. Der Verantwortliche gewährt dem Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen wie in **Annex 1** beschrieben.

3 RECHTE UND PFLICHTEN DES VERANTWORTLICHEN

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Verantwortliche verantwortlich. Der Verantwortliche wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

(2) Der Auftragsverarbeiter wird personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zu der Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Soweit im Hauptvertrag Vereinbarungen zu Leistungsänderungen getroffen wurden, gehen diese den Regelungen in diesem Absatz vor. Soweit keine Vereinbarung zu Leistungsänderungen im Hauptvertrag getroffen wurden, werden Weisungen und Maßnahmen, die eine Abweichung zu den in diesem Vertrag oder im Hauptvertrag festgelegten Leistungen darstellen, als Antrag auf Leistungsänderung behandelt. Zusätzliche Weisungen und Maßnahmen, die über die vertraglich vereinbarten Leistungen hinausgehen, sind –soweit nicht ausdrücklich anders vereinbart- bei Mehraufwand für den Auftragsverarbeiter gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Soweit nicht ausdrücklich anders vereinbart, werden Unterstützungsleistungen des Auftragsverarbeiters nach § 3

(5), (6) und § 4 (4), (5) (7), (8, dort Satz 2), (9), (10, dort Satz 2), (11) dieser Vereinbarung gesondert vergütet.

(4) Der Verantwortliche kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in diesem Vertrag niedergelegten Pflichten durch die Einholung von Auskünften und Abfrage der unter § 3 Abs. 4 angeführten Nachweise beim Auftragsverarbeiter in Hinblick auf die ihn betreffende Verarbeitung kontrollieren. Der Verantwortliche wird vorrangig prüfen, ob die in Satz 1 dieses Absatzes eingeräumte Möglichkeit der Überprüfung ausreicht. Der Verantwortliche kann darüber hinaus auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz vor Ort kontrollieren. Der Verantwortliche kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Vom Verantwortlichen mit der Kontrolle betraute Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Die vom Verantwortlichen mit der Kontrolle betrauten Personen oder Dritte werden dem Auftragsverarbeiter in angemessener Form vorangekündigt und in die Lage versetzt, ihre Legitimation zur Durchführung der Kontrollen nachzuweisen. Dritte im Sinne dieses Absatzes dürfen keine Vertreter von Wettbewerbern des Auftragsverarbeiters sein. Der Verantwortliche wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen.

(5) Dem Auftragsverarbeiter steht es frei, die hinreichende Umsetzung der Pflichten aus diesem Vertrag, insbesondere der technisch-organisatorischen Maßnahmen (§ 5) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch folgende Nachweise zu belegen:

- die Einhaltung genehmigter Verhaltensregeln;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit;
- Eigenerklärung des Auftragsverarbeiters.

(5) Der Verantwortliche wird in Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten unverzüglich und vollständig informieren. Der Verantwortliche wird in Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei der Prüfung möglicher Verstöße und bei Abwehr von Ansprüchen betroffener Personen oder Dritten sowie bei der Abwehr von Sanktionen durch Aufsichtsbehörden zeitnah und umfänglich unterstützen.

4 Rechte und Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich im Rahmen des getroffenen Vertrags und nach Weisung des Verantwortlichen entsprechend der Regelung der Ziffer 3 Abs. (2). Der Auftragsverarbeiter verwendet die personenbezogenen Daten für keine anderen Zwecke und wird die ihm überlassenen personenbezogenen Daten nicht an unberechtigte Dritte weitergeben. Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung der

personenbezogenen Daten des Verantwortlichen befassten Mitarbeiter und andere für den Auftragsverarbeiter tätigen Personen diese personenbezogenen Daten nur auf Grundlage der Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

(2) Der Auftragsverarbeiter gewährleistet, einen unabhängigen, fachkundigen und zuverlässigen Datenschutzbeauftragten zu bestellen, sofern dies von dem anwendbaren Recht der Europäischen Union oder des Mitgliedsstaates, dem der Auftragsverarbeiter unterliegt, gefordert wird.

(3) Den Ort der Datenverarbeitung legen die Parteien in **Annex 1** vor der Datenverarbeitung fest. Änderungen des Orts der Datenverarbeitung werden die Parteien bei Bedarf unter Beachtung der in dieser Vereinbarung festgelegten Form vereinbaren. Eine Datenverarbeitung in sogenannten Drittländern (d.h. Ländern, die keine Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums sind und über kein angemessenes Datenschutzniveau verfügen), wird unter Berücksichtigung der einschlägigen geltenden rechtlichen Bestimmungen der Europäischen Union vorgenommen. Etwaige Einschränkungen bei der Wahl der Gestaltungsmöglichkeiten der Datenübermittlung nach Maßgabe der einschlägigen geltenden rechtlichen Bestimmungen werden die Parteien in **Annex 1** festlegen. Der Verantwortliche wird die Wahl der Gestaltung der Datenübermittlung durch den Auftragsverarbeiter nicht unbillig einschränken und im erforderlichen Umfang mitwirken. Der Auftragsverarbeiter wird bei einer nach **Annex 1** zugelassenen Verwendung der EU-Standardvertragsklauseln diese im Namen und im Auftrag des Verantwortlichen abschließen. Die Vertretungsvollmacht hierfür wird hiermit durch den Verantwortlichen erteilt.

(4) Der Auftragsverarbeiter wird – im vertraglich vereinbarten Umfang unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen - den Verantwortlichen bei der Einhaltung seiner ihm nach den geltenden rechtlichen Bestimmungen obliegenden Pflichten unterstützen. Der Auftragsverarbeiter behält sich vor, bei umfangreicher Inanspruchnahme nach diesem Kapitel 4 die eigene Unterstützungsleistung kostenpflichtig nach vereinbartem Tages-/Stundensatz abzurechnen. Die Bewertung der Schwelle zur „umfangreichen Inanspruchnahme" liegt im billigen Ermessen des Auftragsverarbeiters.

(5) Ist der Verantwortliche gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von personenbezogenen Daten zu geben, so wird der Auftragsverarbeiter den Verantwortlichen darin unterstützen, diese Auskünfte zu erteilen, sofern diese Auskünfte die Datenverarbeitung gemäß diesem Vertrag betreffen. Der Auftragsverarbeiter wird den Verantwortlichen – soweit rechtlich zulässig - über an ihn als Auftragsverarbeiter gerichtete Mitteilungen der Aufsichtsbehörden (z. B. Anfragen, Benachrichtigung über Maßnahmen oder Auflagen) in Verbindung mit der Verarbeitung von personenbezogenen Daten nach diesem Vertrag informieren. Soweit rechtlich zulässig wird der Auftragsverarbeiter Auskünfte an Dritte, auch an Aufsichtsbehörden, nur nach schriftlicher Zustimmung durch und in Abstimmung mit dem Verantwortlichen erteilen.

(6) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

(7) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung.

(8) Der Auftragsverarbeiter führt nach Maßgabe der einschlägigen geltenden rechtlichen Bestimmungen, denen der Auftragsverarbeiter unterliegt, ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung. Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage und stellt dem Verantwortlichen die für die Führung seines Verzeichnisses von Verarbeitungstätigkeiten notwendigen Angaben zur Verfügung, soweit diese Angaben im vertraglich umschriebenen Verantwortungs- und Leistungsbereich als Auftragsverarbeiter liegen und der Verantwortliche keinen anderen Zugang zu diesen Informationen hat.

(9) Falls der Verantwortliche eine Datenschutz-Folgenabschätzung durchführt und/oder eine Konsultation der Aufsichtsbehörde nach einer Datenschutzfolgenabschätzung beabsichtigt, werden sich die Vertragsparteien bei Bedarf über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragsverarbeiters abstimmen.

(10) Abhängig von der Art der Verarbeitung wird der Auftragsverarbeiter den Verantwortlichen bei dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Bei Bedarf werden sich die Vertragsparteien über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragsverarbeiters abstimmen. Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, leitet der Auftragsverarbeiter die Anfragen der betroffenen Person zeitnah an den Verantwortlichen weiter.

(11) Soweit sich Speichermedien im Besitz des Verantwortlichen befinden, wird der Verantwortliche vor einer etwaig vorgesehenen Übergabe (z.B. zur Prüfung oder Abwicklung von Gewährleistungsansprüchen) an den Auftragsverarbeiter oder dessen Unter-Auftragsverarbeiter alle personenbezogenen Daten – soweit nicht anders vereinbart – löschen.

(12) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien, mit Ausnahme der aufgrund gesetzlicher Verpflichtung des Auftragsverarbeiters weiter vorzuhaltenden personenbezogenen Daten, werden – soweit nicht im Hauptvertrag und dessen Anlagen und Anhänge bereits geregelt und soweit nicht anders vereinbart – an den Verantwortlichen zurückgegeben oder auf Kosten des Verantwortlichen vernichtet bzw. gelöscht. Gleiches gilt für Test- und Ausschussmaterial.

(13) Sofern die Vertragsparteien eine ausdrückliche Vereinbarung zur Rückgabe und Löschung von personenbezogenen Daten bzw. Datenträgern getroffen haben, geht diese Vereinbarung den Regelungen in diesem Absatz vor. Soweit die Vertragsparteien keine ausdrückliche Vereinbarung zur Rückgabe von personenbezogenen Daten bzw. Datenträgern des Verantwortlichen getroffen haben kann der Auftragsverarbeiter personenbezogene Daten bzw. Datenträger des Verantwortlichen auf Kosten des Verantwortlichen zurückgeben. Wenn der Verantwortliche seiner Rücknahmepflicht nicht nachkommt, steht es dem Auftragsverarbeiter frei, die personenbezogenen Daten bzw. Datenträger auf Kosten des Verantwortlichen zu löschen/vernichten. Der Verantwortliche kann während des Bestehens des Vertragsverhältnisses oder mit Vertragsende schriftlich die personenbezogenen Daten, die nicht gemäß Abs. ((12) vernichtet bzw. gelöscht sind, auf seine Kosten heraus verlangen und dem Auftragsverarbeiter einen Zeitpunkt (längstens bis Vertragsende) für die Herausgabe nennen. Die Vertragsparteien werden sich nach Herausgabeverlangen auf die weiteren Modalitäten der Herausgabe (wie z.B. Format) verständigen. Das Herausgabeverlangen muss dem Auftragsverarbeiter einen Monat vor dem vom Verantwortlichen benannten Zeitpunkt bzw. ein Monat vor Vertragsende zugegangen sein.

5 TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMAßNAHMEN

(1) Der Verantwortliche und der Auftragsverarbeiter werden geeignete technische und organisatorische Maßnahmen treffen, um ein, dem Risiko angemessenes Schutzniveau zu gewährleisten. Die derzeit als geeignet angesehenen Maßnahmen des Auftragsverarbeiters sind in **Annex 2** beschrieben. Der Verantwortliche hat die technischen und organisatorischen Maßnahmen im Zusammenhang mit etwaigen weiteren Maßnahmen in Hinblick auf ein angemessenes Schutzniveau bewertet. Diese Maßnahmen werden wie in **Annex 2** beschrieben, als geeignete Maßnahmen vereinbart. Etwaige Weiterentwicklungen erfolgen nach Maßgabe von § 5 Abs. 2.

(2) Die technischen und organisatorischen Maßnahmen können im Laufe des Vertragsverhältnisses angepasst werden. Die Sicherheit der Verarbeitung und die Angemessenheit des Schutzniveaus wird der Verantwortliche regelmäßig prüfen und dem Auftragsverarbeiter etwaigen Anpassungsbedarf unverzüglich mitteilen. Der Verantwortliche wird dem Auftragsverarbeiter hierzu alle erforderlichen Informationen zur Verfügung stellen. Der Auftragsverarbeiter seinerseits kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen der DS-GVO. Der Verantwortliche ersetzt dem Auftragsverarbeiter, soweit nicht ausdrücklich anderweitig vereinbart, den durch die Anpassung der Schutzmaßnahmen an den technischen Fortschritt entstehenden Mehraufwand.

(3) Für die Überprüfungs- und Nachweismöglichkeiten gelten Ziffer 3 Abs. (4) und Ziffer 3 Abs. (5).

6 VERTRAULICHKEIT

(1) Der Auftragsverarbeiter wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit wahren. Er wird die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten, soweit diese nicht bereits einer

angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Vereinbarungen im Hauptvertrag zur Wahrung der Vertraulichkeit, die nicht vom Anwendungsbereich dieses Auftragsverarbeitungsvertrags betroffen sind, bleiben unberührt.

(2) Der Auftragsverarbeiter wird Personen, die Zugang zu personenbezogenen Daten haben, mit den für sie maßgeblichen Datenschutzvorgaben und Weisungen dieser Vereinbarung im Voraus vertraut machen.

7 UNTERAUFTRAGSVERARBEITER

(1) Der Auftragsverarbeiter darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einsetzen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Aufträge zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung erteilt und die keine Auftragsverarbeitungsleistung für den Verantwortlichen beinhalten. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind insbesondere Nebenleistungen zu verstehen, die der Anbieter z.B. als Telekommunikationsleistung, Post-/Transportdienstleistung, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahme zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(2) Für die in **Annex 3** aufgeführten Unterauftragsverarbeiter sowie die in **Annex 4** aufgeführten Sub-Unterauftragsverarbeiter und die dort genannten Aufgabenbereiche gilt die Genehmigung des Verantwortlichen als erteilt.

(3) Der Verantwortliche erteilt hiermit dem Auftragsverarbeiter die allgemeine Genehmigung für den künftigen Einsatz weiterer Auftragsverarbeiter (Unterauftrags- und Sub-Unterauftragsverarbeiter) nach Maßgabe des folgenden Absatzes (4).

(4) Der Auftragsverarbeiter informiert den Verantwortlichen schriftlich oder per E-Mail oder auf der Firmenwebsite des Auftragsverarbeiters über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter), wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen binnen 14 Tagen nach Zugang der Information beim Verantwortlichen Einspruch zu erheben. Die Vertragsparteien werden sich bei Bedarf über Art und Weise, hinzutretender oder alternativer Möglichkeiten der Information über den künftigen Einsatz oder Änderungen beim Einsatz weiterer Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter verständigen. Dies kann z.B. die Vorhaltung und den Abruf einer Listung der Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einschließen. Der Verantwortliche wird die Genehmigung zur Einbindung weiterer Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter nicht ohne wichtigen Grund verweigern.

(5) Dem Auftragsverarbeiter steht ein außerordentliches **Kündigungsrecht** des Hauptvertrages nach Maßgabe des Hauptvertrages – oder für den Fall, dass ein solches Kündigungsrecht im

Hauptvertrag nicht eingeräumt wurde, ein außerordentliches Kündigungsrecht von 4 Wochen zum Monatsende – zu, wenn nach Auffassung des Auftragsverarbeiters der Verantwortliche die Einbindung des Unterauftragsverarbeiters und/oder Sub-Unterauftragsverarbeiters ohne wichtigen Grund verweigert.

(6) Der Auftragsverarbeiter wird Unterauftragsverarbeiter auswählen, die hinreichende Garantien dafür bieten, dass die vereinbarten geeigneten **technischen und organisatorischen Maßnahmen** so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Der Auftragsverarbeiter wird mit Unterauftragsverarbeitern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieses Vertrags inhaltlich entsprechen. Der Auftragsverarbeiter wird mit dem Unterauftragsverarbeiter die technischen und organisatorischen Maßnahmen festlegen und die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und dann regelmäßig kontrollieren.

(7) Die Beauftragung von **Sub-Unterauftragsverarbeitern** durch den Auftragsverarbeiter ist nach Maßgabe der Abs. (1) bis Abs. (6) zulässig.

8 VERTRAGSDAUER, KÜNDIGUNG

Diese Vereinbarung gilt für die Dauer der tatsächlichen Leistungserbringung durch den Auftragsverarbeiter. Dies gilt unabhängig von der Laufzeit etwaiger anderer Verträge (insbesondere des Hauptvertrags), die die Parteien ebenfalls bzgl. der Erbringung der vereinbarten Leistungen abgeschlossen haben.

9 ANSPRECHPARTNER

(1) Ansprechpartner beim Auftragsverarbeiter ist:
Ansprechpartner: Jan Schumacher
Funktion: Geschäftsführer
Telefon: 02924 8795645
E-Mail: datenschutz@simplyroot.de

(2) Datenschutzbeauftragter des Auftragsverarbeiters ist:
Datenschutzbeauftragter: Jan Schumacher
Telefon: 02924 8795645
E-Mail: datenschutz@simplyroot.de

(3) Ansprechpartner des Verantwortlichen ist:
Ansprechpartner: _____
Funktion: _____
Telefon: _____
E-Mail: _____

(4) Datenschutzbeauftragter des Verantwortlichen ist:
Datenschutzbeauftragter: _____
Telefon: _____
E-Mail: _____

10 HAFTUNG UND FREISTELLUNG

(1) Der Verantwortliche gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Pflichten bei der Verarbeitung personenbezogener Daten.

(2) Es gelten die Haftungsbeschränkungen aus dem Hauptvertrag. Der Verantwortliche stellt den Auftragsverarbeiter von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragsverarbeiter aufgrund der vom Verantwortlichen beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer rechtswidrigen Verarbeitung der personenbezogenen durch den Auftragsverarbeiter beruht.

11 SONSTIGES

(1) Von der Ungültigkeit einer Bestimmung dieses Vertrags bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

(2) Sämtliche Änderungen dieses Vertrags sowie Nebenabreden bedürfen der Schriftform (einschließlich in elektronischer Form). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

(3) Die Allgemeinen Geschäftsbedingungen des Verantwortlichen finden auf diesen Vertrag keine Anwendung.

(4) Alleiniger Gerichtsstand zu diesem Vertrag ist derjenige des Hauptvertrages. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

(5) Bei Widersprüchen zwischen den Bestimmungen dieses Vertrags und Bestimmungen sonstiger Vereinbarungen, insbesondere des Hauptvertrags, sind die Bestimmungen dieses Vertrags maßgebend. Im Übrigen bleiben die Bestimmungen des Hauptvertrags unberührt und gelten für diesen Vertrag entsprechend.

Annexe:

Nachstehende Annexe sind feste Bestandteile dieser Vereinbarung:

Annex 1: Einzelheiten der Datenverarbeitung
Annex 2: Technische und organisatorische Sicherheitsmaßnahmen
Annex 3: Genehmigte Unterauftragsverarbeiter
Annex 4: Genehmigte Sub-Unterauftragsverarbeiter

Unterschriftenblatt

Für den Verantwortlichen / Auftraggeber:

Ort, Datum	Ort, Datum
Unterschrift	Unterschrift
Name in Druckbuchstaben	Name in Druckbuchstaben
Funktion	Funktion

Für den Auftragsverarbeiter:

Möhnesee, 23.04.2018
Ort, Datum

Unterschrift 18242

JAN SCHUMACHER
Name in Druckbuchstaben

GESCHÄFTSFÜHRER
Funktion

Annex 1

Einzelheiten der Datenverarbeitung

1. Datenkategorien, Datenarten, Zugriffsformen

a. Kategorien betroffener Personen:

- ☐ Beschäftigte
- ☐ Kunden
- ☐ Lieferanten
- ☐ Abonnenten
- ☐ Interessenten

b. Betroffene personenbezogene Daten:

- ☐ Nachname/Vorname
- ☐ Anschrift
- ☐ Geburtsort
- ☐ Familienstand
- ☐ Kontaktdaten (z. B. Telefon, E-Mail)
- ☐ Anschrift
- ☐ Unterschrift
- ☐ Bestandsdaten (z.B. Rechnungsanschrift, Vertragsnummer)
- ☐ Verkehrsdaten (z.B. Anschlusskennung, Standortdaten, Anfang/Ende einer Telefonverbindung, IP)
- ☐ Vertragsstammdaten
- ☐ Personalstammdaten
- ☐ Abrechnungsdaten
- ☐ Kundenhistorie
- ☐ Nationalität
- ☐ Beruf
- ☐ Bankkonto
- ☐ Kontaktdaten Sozialer Netzwerke
- ☐ Versicherungsdaten
- ☐ biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person

c. Zugriff auf personenbezogene Daten

Der Auftragsverarbeiter erbringt Leistungen im Bereich der Wartung, Fernwartung oder IT-Fehleranalyse. Hierbei kann die Möglichkeit, dass der Auftragsverarbeiter Zugriff auf die Daten erhält, nicht ausgeschlossen werden. Hierbei gelten folgende, erweiterte Pflichten:

- Prüfungs- und Wartungsarbeiten an Arbeitsplatzsystemen des Verantwortlichen werden nach Freigabe durch den jeweiligen Berechtigten / betroffenen Mitarbeiter des Verantwortlichen getroffen.
- Es erfolgt eine gesonderte Mitteilung (per Mail/schriftlich) über anstehende Prüfungs- und Wartungsarbeiten durch den Auftragsverarbeiter an den Verantwortlichen vor Beginn der Arbeiten.
- Auf Anforderung des Verantwortlichen informiert der Auftragsverarbeiter, welche Arbeiten wann und von welchen Mitarbeitern des Auftragsverarbeiters durchgeführt werden und wie diese Personen sich dem Verantwortlichen gegenüber identifizieren und authentifizieren werden.
- Über etwaig notwendige Datensicherungsmaßnahmen in den jeweiligen Verantwortungsbereichen des Auftragsverarbeiters/Verantwortlichen werden sich die Vertragsparteien bei Bedarf verständigen, soweit nicht bereits im Hauptvertrag geregelt.
- Der Auftragsverarbeiter wird von den ihm eingeräumten Zugriffsrechten – auch in zeitlicher Hinsicht – so wenig Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

2. Leistungsbeschreibung

Der Gegenstand der Auftragsverarbeitung sowie Art und Zweck ist im Hauptvertrag beschrieben. Im Wesentlichen handelt es sich um folgende Aufgaben durch den Auftragnehmer zum Zwecke der Erbringung von Internet Dienstleistungen bzw zur Erfüllung des Hauptvertrages oder vorvertraglichen Maßnahmen:

- Abrechnung von Dienstleistungen mittels Abrechnungssoftware
- Webhosting und Domainregistrierung
- Websiteerstellung und Pflege
- Betreib eines eMailservers mit Antispam Lösungen und Archiv
- Archivierung von Daten zum Zwecke der Wiederherstellung im Schadenfall
- Suchmaschinenoptimierung (SEO)
- Abwehr von Angriffen und Filterung von Datenpaketen
- Bereitstellung von Serverstrukturen
- Bereitstellung von virtuellen oder dedizieren Servern und deren Wartung
- Überwachung von Diensten und Datenpaketen

3. Verarbeitungsort:

Die Verarbeitung der Daten findet an folgenden Standorten statt:

- DE - 59519 Möhnesee, Zum Haunert 22
- DE - 60314 Frankfurt am Main, Hanauer Landstrasse 300
- DE - 63067 Offenbach am Main, Strahlenbergerstr. 14
- DE - 60388 Frankfurt am Main, Kruppstraße 105
- DE - 90431 Nürnberg, Siegmundstrasse 135
- Innerhalb des IP Netzwerkes vom Auftragsverarbeiters

4. Anforderungen an die Auftragsverarbeitung in Drittländer)

Für die Verarbeitung von personenbezogenen Daten in Drittländern gelten folgende Vorgaben:

Die Auftragsverarbeitung darf grundsätzlich nicht in einem Drittland stattfinden, im Ausnahmefall nur nach schriftlicher Zustimmung des Auftraggebers. Diese Zustimmung gilt für die Zwecke der Abwehr von Angriffen, Bereinigung und Prüfung von Malware, oder Schutz von eMail-Spam für erteilt. Selbstverpflichtung der Auftragnehmer durch EU-US Privacy-Shield.

Annex 2

Technische und organisatorische Sicherheitsmaßnahmen

Präambel:
Dieser Annex konkretisiert die im Vertrag zur Auftragsverarbeitung getroffenen technischen und organisatorischen Maßnahmen. Dabei werden in diesem Zusammenhang insbesondere der aktuelle Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Datenverarbeitung berücksichtigt. Des Weiteren werden die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen beachtet, um ein dem Risiko entsprechendes, angemessenes Schutzniveau für den Schutz personenbezogener Daten zu erreichen.

▪ 1	Vertraulichkeit auf Dauer
Die Sicherstellung der Vertraulichkeit der Datenverarbeitungssysteme gehört zu den Schlüsselelementen moderner Sicherheitsmechanismen und ist Bestandteil der wesentlichen Schutzziele der DS-GVO. Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem auch solche, die zur Zutritts-, Zugriffs- oder Zugangskontrolle gehören. Die in diesem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sollen nämlich eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.	
Maßnahmen zur Sicherstellung der Vertraulichkeit auf Dauer:	
☐	Vertraulichkeitsvereinbarungen mit internen und externen Mitarbeitern
☐	Vertraulichkeitsvereinbarungen mit externen Dienstleistern
☐	Sicherheitsvereinbarungen mit externen Dienstleistern
☐	Einsatz eines umfassenden Datenschutzkonzepts
☐	Einhaltung von Sicherheitsrichtlinien, um Schwachstellen für den Schutz personenbezogener Daten zu ermitteln und die Sicherheitsinfrastruktur zu verwalten
☐	Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle
☐	Schutz vor äußeren Einflüssen (Spionage, Hacking)

☐	Spezifizierte, für die Datenverarbeitungstätigkeit entsprechend dem Datenschutzkonzept ausgestattete Umgebungen (Gebäude, Räume, insb. Server-Räume)
☐	Berücksichtigung der Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Grundeinstellungen (Privacy by Design, Privacy by Default) im Datenschutzkonzept
☐	Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen
☐	Schutzbedarfklassifizierung von zu verarbeitenden personenbezogenen Daten
☐	Zugriffskontrollen (siehe Ziffer 9)
☐	Zutrittskontrollen (siehe Ziffer 10)
☐	Zugangskontrollen (siehe Ziffer 11)
☐	Einsatz von Verschlüsselungsmechanismen (siehe Ziffer 4)
Sonstige Maßnahmen (soweit oben nicht erwähnt):	

2 Integrität auf Dauer

Die Sicherstellung der Integrität der Datenverarbeitungssysteme gehört ebenso, so wie die Sicherstellung der Vertraulichkeit der Datenverarbeitungssysteme, zu den wichtigsten Schutzzielen der DS-GVO. Maßnahmen zur Umsetzung des Gebots der Integrität sind zum einen solche, die auch zur Eingabekontrolle gehören, zum anderen aber solche, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen.

Maßnahmen zur Sicherstellung der Integrität auf Dauer:

☐	Einsatz eines Kryptokonzeptes, aufbauend auf einer risikobasierten Klassifizierung von Datensätzen in Schutzbedarfskategorien
☐	Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß des Kryptokonzeptes
☐	Dokumentieren der Zuweisung von Berechtigungen und Rollen
☐	Prozesse zur Aufrechterhaltung der Aktualität von Daten
☐	Dokumentierung des Hard- und Softwarebestandes und Führung eines Bestandsverzeichnisses
☐	Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
☐	Eingabekontrollen (siehe Ziffer 13)

Sonstige Maßnahmen (soweit oben nicht erwähnt):

3 Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Maßnahmen in Zusammenhang mit der Pseudonymisierung personenbezogener Daten:
☐ Auswahl eines geeigneten Pseudonymisierungsverfahrens nach aktuellem Stand der Technik
☐ Pseudonymisierungsgebot ist zentraler Bestandteil im Rahmen des Datenschutzkonzepts des Unternehmens
☐ Pseudonymisierung von Daten nach einem risikobasierten Ansatz entsprechend unterschiedlichen Schutzbedarfskategorien von Daten
☐ Einsatz von Software, die sicheres Management pseudonymisierter Daten erlaubt
☐ Gesicherte Aufbewahrung der zur Pseudonymisierung verwendeten kryptographischen Schlüssel bzw. Kontrolllisten (ggf. verschlüsselte Speicherung der Kontrolllisten)
☐ Berechtigungskonzept für Zugriff auf kryptographischen Schlüssel bzw. Kontrolllisten, die eine Personalisierung ermöglichen
Sonstige Maßnahmen (soweit oben nicht erwähnt):

4 Verschlüsselung

Die Verschlüsselung personenbezogener Daten ist eine gängige Möglichkeit diese gegen die Kenntnisnahme durch Unbefugte zu schützen. Insbesondere eignet sich die Verschlüsselung dafür, Daten von äußeren Einflüssen wie z.B. Hackangriffe und Spionage zu bewahren. Unter Verschlüsselung ist ein Verfahren zu verstehen, durch das eine klar lesbare Information in eine nicht lesbare bzw. interpretierbare Zeichenabfolge umgewandelt wird.

Maßnahmen in Zusammenhang mit der Verschlüsselung personenbezogener Daten:
☐ Auswahl eines geeigneten kryptographischen Verfahrens erfolgt nach Berücksichtigung des aktuellen Stands der Technik und der Schutzbedarfskategorien der zu verarbeitenden personenbezogenen Daten
☐ Einsatz von Verschlüsselungsverfahren entsprechend dem Datenschutzkonzept
☐ Regelmäßige Prüfung der Verschlüsselungsverfahren (insb. auf Sicherheitslücken) und Anpassung dieser an die aktuellen technischen Entwicklungen (insb. Aktualisierung der eingesetzten Software)

☐ Regelmäßige Aufbereitung von archivierten verschlüsselten Daten nach dem neuesten Stand der Technik (insb. beim Einführen von neuen Verschlüsselungsverfahren bei der Datenverarbeitungstätigkeit)
☐ Verschlüsselungsrichtlinien berücksichtigen die unterschiedlichen Schutzkategorien personenbezogener Daten
☐ Löschung der Ursprungsdatei nach erfolgreicher Verschlüsselung; bei WORM-Medien Vernichtung der gesamten Datenträger
☐ Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (insbesondere Berechtigungskonzept für interne und externe Mitarbeiter, die Zugang zu verschlüsselte Informationen haben)
☐ Schulung von internen und externen Mitarbeitern im Umgang mit verschlüsselten personenbezogenen Daten (mindestens zweimal im Jahr)
Sonstige Maßnahmen (soweit oben nicht erwähnt):

5	Verfügbarkeit auf Dauer
Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten.	
Maßnahmen zur Sicherstellung der Verfügbarkeit auf Dauer:	
☐ Zentrale Beschaffung von Hard- und Software	
☐ Einsatz zentral geprüfter und freigegebener Standardsoftware aus sicheren Quellen	
☐ Regelmäßige Durchführung von Datensicherungen bzw. Einsatz von Spiegelungsverfahren	
☐ Außerbetriebnahme von Hardware (insb. von Servern) erfolgt nach einer Überprüfung der darin eingesetzten Datenträger und ggf. nach erfolgter Sicherung der relevanten Datensätze	
☐ Unterbrechungsfreie Stromversorgung (USV)	
☐ Getrennte Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden oder die zu unterschiedlichen Schutzbedarfskategorien gehören	
☐ Mehrschichtige Virenschutz- und Firewall-Architektur	
☐ Notfallplanung (Notfallplan für Sicherheits- und Datenschutzverletzungen mit konkreten Handlungsanweisungen)	
☐ Feuer-/Wasser- und Temperaturfrühwarnsystem in den Serverräumen	
☐ Brandschutztüren	
☐ Betreuung der IT durch qualifizierte und ständig weitergebildete Mitarbeiter	

☐ Regelmäßiges Testen der Datenwiederherstellung entsprechend des Datenschutzkonzepts
Sonstige Maßnahmen (soweit oben nicht erwähnt):

6	Gewährleistung der Belastbarkeit der Systeme auf Dauer

Hierzu gehören beispielsweise Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch den Auftragsverarbeiter zu ergreifen sind. Darüber hinaus ist auch eine kontinuierliche Überwachung der Systeme erforderlich.

Maßnahmen zur Sicherstellung der Belastbarkeit der Systeme und Dienste auf Dauer:
☐ Load-Balancing
☐ Dynamische Prozesse und Speicherzuschaltung
☐ Penetrationstests
☐ Regelmäßige Belastungstests der Datenverarbeitungssysteme
☐ Belastungsgrenze für das jeweilige Datenverarbeitungssystem im Voraus über das notwendige Minimum ansetzen
☐ Regelmäßige Schulung des eingesetzten Personals (Management und sonstige interne und externe Mitarbeiter) entsprechend dem Gebot zur Sicherstellung der Integrität und Vertraulichkeit der Datenverarbeitung zu handeln (mindestens einmal im Jahr)
Sonstige Maßnahmen (soweit oben nicht erwähnt):

7	Wiederherstellbarkeit der Verfügbarkeit

Zur Sicherstellung der Wiederherstellbarkeit sind einerseits ausreichende Sicherungen erforderlich, wie aber auch Maßnahmenpläne, die im Sinne von Katastrophen-Fall-Szenarien (ggf. auch Basis der Sicherungen) den laufenden Betrieb wiederherstellen können.

Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit bei einem physischen oder technischen Zwischenfall:
☐ Regelmäßige Archivierung der Datenbestände und Einsatz von Spiegelungsverfahren
☐ Getrennte Aufbewahrung von Datenbeständen

☐ Maßnahmenplan für Datenpannen (Data Breach Management Plan)
☐ Regelmäßiges Testen der Datenwiederherstellungstools
☐ Notstromversorgung
☐ Zwei voneinander unabhängige Zugangsmöglichkeiten zum externen Netz (Internetzugänge von mindestens zwei unterschiedlichen Providern)
☐ Verfügbarkeit von Back-Up-Rechnern und Software-Lösungen für Notfallsituationen
Sonstige Maßnahmen (soweit oben nicht erwähnt):

8 Überprüfung und Bewertung der Datensicherheit

Maßnahmen um insbesondere die schon getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit laufend aktuell zu halten und kritisch zu begutachten. Diese Pflicht erstreckt sich auf alle technischen und organisatorischen Maßnahmen (Ziff. 1 bis 15).

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:
☐ Interne und externe Prüfberichte und Evaluierungen
☐ Regelmäßige Bewertung von Prüfergebnissen und Anpassungsmaßnahmen vornehmen
☐ Regelmäßige Überprüfung des Hard- und Softwarebestandes entsprechend einem Bestandsverzeichnis und jährliche Aktualisierung des Bestandsverzeichnisses
☐ Regelmäßige Überprüfung von Datenverarbeitungssystemen und Verarbeitungstätigkeiten auf Sicherheitslücken, die aufgrund neuer technischer Entwicklungen oder veränderter Verarbeitungspraxis entstehen können
☐ Regelmäßige Versionskontrolle von Standardsoftware entsprechend dem Datenschutzkonzept (Intensität der Kontrolle hängt von der eingesetzten Software ab, Prüfung soll jedoch mindestens einmal jährlich erfolgen)
☐ Regelmäßiger Abgleich der Schutzbedarfklassifizierung der zu verarbeitenden personenbezogenen Daten mit ggf. neuen Anforderungen des Verantwortlichen
Sonstige Maßnahmen (soweit oben nicht erwähnt):

9 Zugriffskontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Der Auftragsverarbeiter muss deswegen Maßnahmen ergreifen, die dafür Sorge tragen, dass Personen im Rahmen der Datenverarbeitung nur auf die Daten zugreifen können, für die sie über eine entsprechende Berechtigung verfügen und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen zur Verwehrung des Zugriffs auf personenbezogene Daten für Unbefugte:

- ☐ Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen
- ☐ Vorgabe zur Festlegung von Passwörtern (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- ☐ Verbot der Weitergabe von Passwörtern
- ☐ Berechtigungskonzept auf Applikations- und Datenebene mit differenzierten Berechtigungsstufen (Profile, Rollen, Transaktionen und Objekte)
- ☐ Protokollierung der vergebenen Zugriffsberechtigungen
- ☐ Einsatz von Signaturen und Zertifikaten zur Sicherstellung von Urheberschaft und Berechtigung zur Kenntnisnahme
- ☐ Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit
- ☐ Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken entsprechend Schutzklassenkonzept
- ☐ Verbot des Einsatzes privater Datenträger
- ☐ Richtlinie für das Kopieren von Daten
- ☐ Zugriffsschutz durch Bildschirmschoner

Sonstige Maßnahmen (soweit oben nicht erwähnt):

10 Zutrittskontrolle

Damit sind Maßnahmen gemeint, die Unbefugten den Zutritt zu den Gebäuden und Rechenzentren verwehren, in denen personenbezogene Daten verarbeitet werden. Der Auftragsverarbeiter ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass nur die Personen Zutritt zu den Gebäuden und Rechenzentren haben, die über eine entsprechende Berechtigung verfügen.

Maßnahmen zur Verwehrung des Zutritts zu Datenverarbeitungsanlagen für Unbefugte:
☐ Festlegung zutrittsberechtigter Personen
☐ Zutrittskontrolleinrichtungen unter Einsatz personalisierter und codierter Ausweiskarten mit Lichtbild
☐ Zutrittsregelung für betriebsfremde Personen
☐ Einrichtung verschiedener Sicherheitszonen mit verschiedenen Zutrittsberechtigungen
☐ Dokumentation der Vergabe und des Entzugs von Zutrittsberechtigungen
☐ Einbruchsmeldeanlage mit Alarmübertragung zur ununterbrochen besetzten Sicherheitsleitstelle bzw. zur Polizei
☐ Zusätzliche Zutrittskontrollmaßnahmen sowie Türzustandsüberwachung für Serverräume
☐ Fluchttürüberwachung
☐ Restriktive Schlüsselregelungen
☐ Besucheraufenthalte nur in Begleitung von Beschäftigten des Auftragsverarbeiters
☐ Ausweistragepflicht
☐ Videoaufzeichnung in bestimmten Bereichen
☐ Videoüberwachung der Zugänge
☐ Biometrische Zugangssperren (z.B. zu Server-Räumen)
Sonstige Maßnahmen (soweit oben nicht erwähnt):

11	Zugangskontrolle zu Datenverarbeitungssysteme

Damit sind Maßnahmen gemeint, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen. Der Auftragsverarbeiter muss in diesem Zusammenhang Maßnahmen ergreifen, die dafür Sorge tragen, dass nur Personen auf Anlagen zur Datenverarbeitung zugreifen können, die über eine entsprechende Berechtigung verfügen. Hierzu gehören bspw. geeignete Passwortregeln und Firewallkonfigurationen.
Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:
☐ Kennwortverfahren (u.a. Festlegungen hinsichtlich Verwendung von Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)

☐ Bios-Passwörter
☐ Verbot der Weitergabe von Kennwörtern
☐ Automatische Sperrung des Bildschirms bei Inaktivität nach Zeit
☐ Sperren von Arbeitsplätzen und/oder Benutzernamen bei mehrfachen fehlerhaften Zugriffsversuchen
☐ Regelmäßige Zugangsberechtigungsprüfungen
☐ Protokollierung der Nutzung von Zugangsberechtigungen
☐ Abschottung interner Netzwerke durch Einrichtung von Firewall-Systemen
☐ Verschlüsselung von Daten und Festplatten gemäß Schutzklassenkonzept
☐ Verschlüsselung von Smartphones
☐ Gehäuseverriegelungen
Sonstige Maßnahmen (soweit oben nicht erwähnt):

12	Weitergabekontrolle

Damit sind Maßnahmen gemeint, 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.

Maßnahmen zur Verwehrung der unbefugten Kenntnisnahme, der Nachvollziehbarkeit und Wahrung der Integrität bei der Datenübertragung:
☐ Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit insbesondere mittels Datei- und Festplattenverschlüsselung auf Hard- oder Softwarebasis (z.B. Secude Secure File, SecureDoc Disk Encryption, Truecript)
☐ Verschlüsselung der Übertragung von Daten, insbesondere bei der Übertragung über öffentliche Netze (z.B. ssl, tls)
☐ Verwendung von Virtual Private Networks (VPN)
☐ Benutzung verschließbarer Transportbehälter
☐ Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken entsprechend Schutzklassenkonzept

☐ Elektronische Signatur
☐ Sorgfältige Auswahl von Transportpersonal
Sonstige Maßnahmen (soweit oben nicht erwähnt):

13 Eingabekontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-Systemen bzw. -Anwendungen eingegeben, verändert oder entfernt worden sind.

Maßnahmen zur nachträglichen Überprüfung und Nachvollziehbarkeit bei Eingaben, Änderungen und Löschungen:
☐ Gesetzeskonforme Vertragsgestaltung von Verträgen über die Datenverarbeitung personenbezogener Daten mit Subunternehmern mit entsprechender Regelung von Kontrollmechanismen
☐ Einholung von Selbstauskünften bei Dienstleistern bezüglich deren Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen
☐ Anschließende Bestätigung von mündlichen Weisungen in Text- oder Schriftform
☐ Aufzeichnung und bedarfsgerechtes Vorhalten von entsprechenden, an Systemen durchgeführten Aktionen (z.B. Logfiles)
☐ Einsatz von Protokollierungs- und Protokollauswertungssysteme
☐ Festlegung der Befugten für die Erstellung von Datenträgern und der Bearbeitung von Daten
Sonstige Maßnahmen (soweit oben nicht erwähnt):

14 Auftragskontrolle (bei Einsatz von Subunternehmern)

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten, die im Auftrag bei einem Subunternehmer des Auftragsverarbeiters verarbeitet werden, nur entsprechend den Weisungen und Anforderungen an die Datenverarbeitung des Auftraggebers verarbeitet werden können.
Maßnahmen zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur nach Weisung des Auftraggebers verarbeitet werden:
☐ Kriterien zur Auswahl der Auftragnehmer festgelegt (Referenzen, Zertifizierungen, Gütesiegel)

☐ Detaillierte schriftliche Regelungen (Vertrag/Vereinbarung) der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes, auch zum Einsatz von Subunternehmern, eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten
☐ Sicherstellung, dass die Auftragsdurchführung kontrolliert und dokumentiert wird
☐ Vereinbarung von Vertragsstrafen (mit Subunternehmern) für Verstöße gegen erteilte Weisungen
☐ Vertragliche Vereinbarung mit Subunternehmern eigene und externe Mitarbeiter auf das Datengeheimnis zu verpflichten
Sonstige Maßnahmen (soweit oben nicht erwähnt):

15	Trennungskontrolle
Damit sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	
Maßnahmen zur Trennnungskontrolle:	
☐ Logische bzw. technische Trennung von Daten	
☐ Benutzerprofile / Trennung von Nutzerkonten	
☐ Unterschiedliche Zugriffsberechtigungen	
☐ Speicherung in spezifischen Speicherbereichen	
☐ Trennung der verarbeitenden Systeme	
Sonstige Maßnahmen (soweit oben nicht erwähnt):	

Annex 3

Angaben zu Unterauftragsverarbeitern

Die folgenden Unterauftragsverarbeiter dürfen im Rahmen der Vereinbarungen gem. Annex 2 eingesetzt werden und bestehen zum Zeitpunkt des Vertragsschlusses zwischen den Parteien.

1. webhoster.de AG, Zum Haunert 22, 59519 Möhnesee

Datenschutzbeauftragter: Jan Schumacher, datenschutz@webhoster.ag

Leistungen: Internet Dienstleistungen, Webhosting, Domainregistrierung, Suchmaschinenoptimierung, Websitepflege, Sicherheitsdienstleistungen, Wartung und Support, Abrechnung

2. Key-Systems GmbH, Im Oberen Werk 1, 66386 St. Ingbert

Datenschutzbeauftragter: sales@key-systems.net

Leistungen: Registrar-Dienstleistungen für Domainregistrierungen

Verarbeitungsort: Im Oberen Werk 1, 66386 St. Ingbert

Annex 4

Genehmigte Sub-Unterauftragsverarbeiter

1. Ecotel AG, Hanauer Landstrasse 300, 60314 Frankfurt am Main

Datenschutzbeauftragter: noc@ecotel.de

Leistungen: Erbringung von Datacenter Leistungen, Lieferung von Strom, Routing von IP Datentransfer.

Verarbeitungsort: Hanauer Landstrasse 300, 60314 Frankfurt am Main

2. Aixit GmbH, Strahlenbergerstr. 14, 63067 Offenbach am Main

Datenschutzbeauftragter: service@aixit.com

Leistungen: Erbringung von Datacenter Leistungen, Lieferung von Strom, Routing von IP Datentransfer.

Verarbeitungsort: Strahlenbergerstr. 14, 63067 Offenbach am Main

3. Accelerated IT Services GmbH, Kruppstraße 105, 60388 Frankfurt am Main

Datenschutzbeauftragter: info@accelerated.de

Leistungen: Erbringung von Datacenter Leistungen, Lieferung von Strom, Routing von IP Datentransfer.

4. Hetzner Online GmbH, Siegmundstrasse 135, 90431 Nürnberg

Datenschutzbeauftragter: support@hetzner.com

Leistungen: Erbringung von Datacenter Leistungen, Lieferung von Strom, kein Routing von IP Datentransfer

Verarbeitungsort Siegmundstrasse 135, 90431 Nürnberg

5. CPS Datensysteme GmbH, Gilgenborn 44, 56179 Vallendar

Datenschutzbeauftragter: de.support@cps-datensysteme.de

Leistungen: Registrar-Dienstleistungen für Domainregistrierungen

Verarbeitungsort Gilgenborn 44, 56179 Vallendar

6. Hexonet GmbH, Talstrasse 27, 66424 Homburg

Datenschutzbeauftragter: help@hexonet.support

Leistungen: Registrar-Dienstleistungen für Domainregistrierungen

Verarbeitungsort Talstrasse 27, 66424 Homburg

7. Internexum GmbH, Blumenstr. 54, 02826 Görlitz

Datenschutzbeauftragter: support@nicmananger.de

Leistungen: Registrar-Dienstleistungen für Domainregistrierungen

Verarbeitungsort: Blumenstr. 54, 02826 Görlitz

8. Nic.at GmbH, Jakob-Haringer-Str. 8/V, 5020 Salzburg, AT

Datenschutzbeauftragter: support@nicmananger.de

Leistungen: Registrar-Dienstleistungen für Domainregistrierungen

Verarbeitungsort: Jakob-Haringer-Str. 8/V, 5020 Salzburg, AT

9. Internetx GmbH, Johanna-Dachs-Str. 55, 93055 Regensburg

Datenschutzbeauftragter: info@internetx.de

Leistungen: Registrar-Dienstleistungen für Domainregistrierungen

Verarbeitungsort: Johanna-Dachs-Str. 55, 93055 Regensburg

10. Cloudflare Inc. 101 Townsend St. San Francisco, CA 94107, USA

Datenschutzbeauftragter: privacy@cloudflare.com

Leistungen: bei Bedarf: Web Beschleunigung, Schutz vor Angriffen, DNS

11. SiteLock, 8701 E Hartford Drive, Suite 200, Scottsdale, AZ 85255, USA

Datenschutzbeauftragter: info@sitelock.com

Leistungen: Malware und Virusbereinigung von Dateien, Firewall zum Schutz vor Angriffen.

12. Spamexperts B.V., Rokin 113-115, 1012 KP Amsterdam, NL

Datenschutzbeauftragter: MSPlegal@solarwinds.com

Leistungen: eMailanalyse, eMailarchivierung, Antispam Dienstleistungen

13. Imperva Inc., 3400 Bridge Parkway, Suite 200, Redwood Shores, CA 94065, USA

Datenschutzbeauftragter: support@imperva.com

Leistungen: Web Beschleunigung, Schutz vor Angriffen, DNS

14. Agentur Ehrenwert UG, Zum Haunert 22, 59519 Möhnesee

Datenschutzbeauftragter: Jan Schumacher, datenschutz@ehrenwert.it

Leistungen: Internet Dienstleistungen, Webhosting, Domainregistrierung, Suchmaschinenoptimierung, Websitepflege, Sicherheitsdienstleistungen, Wartung und Support, Abrechnung

15. TecServer GmbH, Zum Haunert 22, 59519 Möhnesee

Datenschutzbeauftragter: Jan Schumacher, datenschutz@tecserver.com

Leistungen: Internet Dienstleistungen, Webhosting, Domainregistrierung, Suchmaschinenoptimierung, Websitepflege, Sicherheitsdienstleistungen, Wartung und Support, Abrechnung

16. iSearch GmbH, Zum Haunert 22, 59519 Möhnesee

Datenschutzbeauftragter: Jan Schumacher, datenschutz@isearch.de

Leistungen: Internet Dienstleistungen, Suchmaschinenoptimierung, Websitepflege, Sicherheitsdienstleistungen, Wartung und Support, Werbung, Abrechnung

17. iStore UG, Zum Haunert 22, 59519 Möhnesee

Datenschutzbeauftragter: Jan Schumacher, datenschutz@istore.de

Leistungen: Suchmaschinenoptimierung, Websitepflege, Sicherheitsdienstleistungen, Wartung und Support, Abrechnung

18. Apple Inc., Infinite Loop, Cupertino, CA 95014, USA

Datenschutzbeauftragter: contactus.de@euro.apple.com

Leistungen: Arbeitscomputer, Cloudspeicher, Verwaltung, Abrechnung

19. Partnergate GmbH, Wilhelm-Wagenfeld-Str. 16, 80807 München

Datenschutzbeauftragter: Christian Ambil, ca@partnergate.de

Leistungen: Registrar-Dienstleistungen für Domainregistrierungen

20. Barracuda Networks Inc., 3175 Winchester Blvd, Campbell, CA 95008, USA

Datenschutzbeauftragter: legal@barracuda.com

Leistungen: eMailanalyse, eMailarchivierung, Antispam Dienstleistungen

21. TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen

Datenschutzbeauftragter: service@teamviewer.com

Leistungen: Fernwartung von Computersystemen, Service, Kommunikation