Vereinbarung
über die Verarbeitung personenbezogener Daten (Auftragsverarbeitung)

zwischen

Name: . . . . . .
Straße: . . . . . .
PLZ Ort: . . . . . .

- nachstehend Auftraggeber genannt -

und

Name: casusbene GmbH
Straße: Hainhölzer Str. 5
PLZ Ort: 30159 Hannover

- nachstehend Auftragnehmer genannt -

- nachstehend einzeln oder gemeinsam auch Parteien genannt -

Diese Vereinbarung konkretisiert die gesetzlichen Rechte und Pflichten, die sich für die Vertragsparteien aus dem anwendbaren Datenschutzrecht und insbesondere aus dem Bundesdatenschutzgesetz, ab dem 25.05.2018 aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DS-GVO“) sowie der nationalen Datenschutzgesetze ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet (Anlage 1). Sie findet Anwendung auf alle Tätigkeiten, die mit dem/den Hauptvertrag/Hauptverträgen (im Einzelnen in Anlage 1 aufgeführt) in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Als solche Tätigkeiten kommen insbesondere ein Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/ Backup-Datei – vor allem im Zusammenhang mit Supportanfragen – in Betracht, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Hauptverträge. Sie endet, ohne dass es einer gesonderten Kündigung bedarf mit dem Laufzeitende des letzten verbleibenden, in Anlage 1 aufgeführten Hauptvertrages.

§ 1 Definitionen

(1) Personenbezogene Daten: Personenbezogene Daten sind 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) Verarbeitung: Verarbeitung umfasst 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.

(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete dokumentierte Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in dokumentierter Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich

(1) Der Auftragnehmer prüft und wartet automatisierte Verfahren oder Datenverarbeitungsanlagen im Auftrag, insbesondere die von ihm im Rahmen eines getrennten Vertragsverhältnisses überlassene Standardsoftware und bietet im Rahmen seiner Supportangebote weitergehende Hilfestellungen im Umgang mit der Software an. Ferner bietet er Softwarelösungen auch im Rahmen von Hosting, ASP, SaaS oder Cloud basierender Angebote an. Im Rahmen dieser Tätigkeiten kann in besonderen Konstellationen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Die umfassten Tätigkeiten sind in der Leistungsbeschreibung des Hauptvertrages konkretisiert. Die Hauptverträge sind ferner in Anhang 1 zu dieser Vereinbarung, unter Nennung der jeweils betroffenen Datenkategorien, aufgeführt. Die Auflistung wird von den Parteien bei Wegfall oder Neuabschluss eines weiteren Hauptvertrages, der auch Auftragsverarbeitung zum Gegenstand hat, fortlaufend aktualisiert.

(2) Die nach diesem Vertrag den Parteien auferlegten Rechte und Pflichten gelten nur während der Laufzeit des Vertrages und innerhalb dieses Zeitraums nur in den Zeitabschnitten bei denen tatsächlich eine Auftragsverarbeitung durchgeführt wird oder eine vergleichbare Gefahrenlage für personenbezogene Daten, für die der Auftraggeber verantwortliche Stelle ist, gegeben ist.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Darüber hinaus kann sich im Einzelfall für den Auftragnehmer eine gesetzliche Verpflichtung zur Verarbeitung personenbezogener Daten ergeben. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die betreffende rechtliche Verpflichtung verbietet eine solche Mitteilung wegen wichtigen öffentlichen Interesses.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so

gestalten, dass sie den besonderen Anforderungen des anwendbaren Datenschutzrechts gerecht wird. Er wird die geeigneten und gesetzlich erforderlichen technischen und organisatorischen Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet insbesondere

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird als Anlage 2 diesem Vertrag beigefügt.

(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

(4) Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.

(5) Im Rahmen des Zumutbaren und Erforderlichen sowie unter Berücksichtigung der Art der Verarbeitung und der vorliegenden Informationen unterstützt der Auftragnehmer den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der gesetzlichen Pflichten, die den Auftraggeber als Verantwortlichen treffen (u.a. bei der Wahrnehmung von Betroffenenrechten, der Durchführung von Kontrollen durch die zuständige Datenschutzaufsichtsbehörde sowie bei der Erfüllung gesetzlicher Informationspflichten gegenüber Betroffenen und Datenschutzbehörden). Der Auftraggeber erstattet dem Auftragnehmer durch die Unterstützung entstehende Kosten und Aufwand. Können sich die Parteien nicht über den Umfang der Erstattung einigen, werden die Kosten, die der Auftragnehmer für erforderlich halten durfte, in vollem Umfang erstattet.

(6) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(7) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und auf Verlangen in geeigneter Weise nachzuweisen.

(8) Die Auftragsverarbeitung darf nur innerhalb des Gebiets eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden. Eine Verlagerung in ein Drittland außerhalb dieses Gebietes bedarf der vorherigen Zustimmung des Auftraggebers.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne des anwendbaren Datenschutzrechts für die Verarbeitung von Daten im

Auftrag durch den Auftragnehmer verantwortlich (Verantwortlicher). Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber.

(2) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen (Einzelweisung). Der Auftraggeber trägt hierdurch anfallende Mehrkosten; der Auftragnehmer kann einen Vorschuss verlangen. Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer erheblichen Änderung des Arbeitsaufwands führen würden oder wenn der Auftraggeber die Erstattung der Mehrkosten oder den Vorschuss verweigert.

(3) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund von angeblich unrechtmäßigen Datenverarbeitungen Ansprüche geltend machen, wird der Auftraggeber, soweit diese angeblich unrechtmäßigen Verarbeitungen auf Vorsatz oder Fahrlässigkeit des Auftraggebers beruhen, den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen. Soweit der Auftragnehmer den Auftraggeber bei der Erfüllung der Ansprüche Betroffener unterstützt (insbesondere hinsichtlich Berichtigung, Löschung und Sperrung von Daten), erstattet der Auftraggeber dem Auftragnehmer Kosten und Aufwand. Die Parteien verständigen sich über den erwarteten Umfang von Kosten und Aufwand.

(4) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 5 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Die hierfür erforderlichen Informationen werden dem Auftraggeber gemäß nachfolgendem Absatz zur Verfügung gestellt.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag geregelten Pflichten zur Verfügung. Er ermöglicht und trägt bei zu Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

(3) Die Häufigkeit der Kontrollen soll, maximal einmal jährlich erfolgen. Hiervon unbenommen ist das Recht des Auftraggebers, anlassbezogen weitere Kontrollen im Fall von Verletzungen datenschutzrechtlicher Pflichten durch den Auftragnehmer durchzuführen.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt durch eine Vor-Ort Kontrolle durch die Vorlage eines geeigneten Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revisor, interner oder externer Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor) oder einer geeigneten Datenschutz-Zertifizierung durch eine zugelassene Stelle erbracht werden ("Zertifizierungsurkunde"). Die Zertifizierungsurkunde muss es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß beiliegender Anlage 2 zu überzeugen.

§ 7 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen die in der Anlage 3 benannten weiteren Auftragsverarbeiter (Subunternehmer)

einschaltet. Über eine Änderung der in der Anlage 3 genannten Subunternehmer wird der Auftragnehmer den Auftraggeber informieren und ihm die Möglichkeit geben, gegen derartige Änderungen einen Einspruch zu erheben.

(2) Im Übrigen ist die Beauftragung von Subunternehmern durch den Auftragnehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig. Die Zustimmung darf nur aus wichtigem, dem Auftragnehmer nachzuweisendem Grund verweigert werden. Im Fall der Einschaltung von im Sinne der §§ 15 ff. AktG mit dem Auftragnehmer verbundenen Unternehmen als Subunternehmer erteilt der Auftraggeber hiermit schon jetzt ausdrücklich seine Zustimmung.

(3) Der Auftragnehmer wird weiteren Auftragsverarbeitern vertraglich dieselben Pflichten wie nach diesem Vertrag auferlegen, einschließlich hinreichender Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten, datenschutzbezogenen Vertragsunterlagen.

§ 8 Informationspflichten

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

§ 9 Vertragsdauer und -beendigung

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des letztbestehenden Hauptvertrages.

(2) Nach Abschluss der Erbringung der Verarbeitungstätigkeiten bzw. nach Beendigung der Vereinbarung hat der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten zu löschen oder herauszugeben. Dies gilt nicht, soweit für den Auftragnehmer auf Grundlage des anwendbaren Datenschutzrechts eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z.B. gesetzliche Aufbewahrungspflicht).

(3) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Dadurch resultierende zusätzliche Kosten durch die Herausgabe oder Löschung der Daten sind vom Auftraggeber zu tragen.

§ 10 Schlussbestimmungen

(1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DS-GVO und/oder der jeweils nationalen Datenschutzgesetze – einvernehmlich anzupassen und zu ändern.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts sowie der Verweisungsnormen des internationalen Privatrechts. Ausschließlicher Gerichtsstand ist Hannover.

(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Ort, Datum _____

_____
Auftraggeber

Ort, Datum _____

_____
casusbene GmbH

Anlage 1
Umfang, Art und Zweck der Datenverarbeitung

I. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien:

- ☐ Hosting von Server-Systemen und dort betriebenen Anwendungen (Datenbank-, Backup-, Web-Server, SAN-Umgebung)
- ☐ Technische Administration der beim Hosting benötigten IT-Systeme
- ☐ Sonstige Support-Tätigkeiten für sämtliche Server-Systeme

Darunter fallen zum Beispiel nachfolgende Daten:

- ☐ Nutzungsdaten (Protokollierung der Nutzeraktivitäten, Log-Files, IP-Adressen)
- ☐ Beschäftigtendaten (Fotos, Namen, Kontaktdaten, Geburtsdaten, Personaldaten, Kontodaten)
- ☐ Kundendaten (Anschriften, Kontaktdaten, Bestelldaten, Umsätze, Kontodaten)
- ☐ Vertragsdaten
- ☐ E-Mails
- ☐ PDF-Downloads

II. Kreis der Betroffenen

Die übertragenen personenbezogenen Daten betreffen die folgenden Personengruppen:

- ☐ Beschäftigte und ehemalige Beschäftigte des Auftraggebers
- ☐ Webseitenbesucher
- ☐ Kunden und Interessenten des Auftraggebers
- ☐ Lieferanten
- ☐ Ansprechpartner
- ☐ Interessenten
- ☐ Handelspartner
- ☐ Abonnenten/ Mitglieder
- ☐ E-Mail-Kontakte

- ☐ Bewerber
- ☐ Sonstige betroffene Personen (Kategorien):

III. Gegenstand und Zweck der Datenverarbeitung

a. Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- ☐ Hosting von Server-Systemen und dort betriebenen Anwendungen (Datenbank-, Backup-, Web-Server, SAN-Umgebung)
- ☐ Technische Administration der beim Hosting benötigten IT-Systeme
- ☐ Sonstige Support-Tätigkeiten für sämtliche Server-Systeme

b. Im Zuge der Leistungserbringung zum Zwecke des Hostings kann ein Zugriff auf personenbezogene Daten durch den Auftragnehmer nicht ausgeschlossen werden. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Bei der Auftragsleistung handelt es sich um folgende Arten der automatisierten Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen:

- ☐ Erheben (z.B. durch Importieren von Daten des Auftraggebers)
- ☐ Speichern (z.B. durch Sicherung und Archivierung auf Festplatten, anderen Speichersystemen oder Datenträgern)
- ☐ Verändern (z.B. durch Änderungen der Benutzer an den Datensätzen)
- ☐ Übermitteln (z.B. durch Übermittlung per E-Mail von Nachrichten)
- ☐ Einschränken (z.B. durch Deaktivierung von einzelnen Datensätzen)
- ☐ Löschen (z.B. durch Vernichten von Datenträgern oder Papierunterlagen)

Anlage 2

Maßnahmen Hosting (Rechenzentrum)

Um die von ihm verarbeiteten personenbezogenen Daten zu schützen, hat der Auftragnehmer bzw. deren Hoster die Mittwald CM Service GmbH & Co. KG angemessene technische und organisatorische Sicherheitsmaßnahmen, einschließlich der folgenden Maßnahmen umgesetzt:

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Das Betriebsgebäude ist in unterschiedliche Zutrittsbereiche eingeteilt.
- Besucher melden sich am Empfang und werden vom Ansprechpartner abgeholt.
- Der Zutritt zu sämtlichen Datenverarbeitungsanlagen ist Unbefugten vollständig verwerht.
- Der Zutritt jeglicher Personen (auch mitarbeiter) muss durch autorisiertes Personal im Voraus genehmigt werden und wird durch eine Personenkontrolle überprüft.
- Sämtliche Zugänge und Räumlichkeiten der Datenverarbeitungsanlagen werden durch Kameras überwacht und durch elektronische Schließsysteme kontrolliert.
- Jeglicher Zutritt wird protokolliert.

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

- Zugang zu den Datenverarbeitungsanlagen erhält ausschließlich autorisiertes und fachlich qualifiziertes Personal.
- Der Zugang erfolgt über eine Benutzerkennung und Eingabe eines Passwortes.
- Die Passwörter entsprechen einem technisch sicheren Niveau und sind durch interne Richtlinien geregelt.
- Die Anmeldungen werden protokolliert.

1.3 Zugriffskontrolle

Es ist sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.

- Der Zugriff auf die Datenverarbeitungssysteme ist durch eine Nutzer- und Rechteverwaltung abgesichert. Es ist dem einzelnen Mitarbeiter nur möglich die für seine Aufgaben erforderlichen

Daten einzusehen, zu nutzen, zu verarbeiten oder zu löschen.

- Die Zugriffe auf die Datenverarbeitungssysteme werden geloggt.
- Beim Verlassen des Arbeitsplatzes erfolgt eine Sperrung durch Bildschirmschoner, Freigabe nur durch Eingabe des Passworts.
- Jeder Mitarbeiter wird entsprechend zur Vertraulichkeit und der Einhaltung des Datenschutzes bei Aufnahme seiner Tätigkeit verpflichtet. Ein Verstoß hätte die fristlose Kündigung, sowie eine Strafanzeige zur Folge. Betroffene Auftraggeber würden in so einem Fall selbstverständlich über den Vorfall informiert.

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Der Auftragnehmer überträgt von sich aus personenbezogene Daten ausschließlich elektronisch über verschlüsselte Datenverbindungen, so dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Eine elektronische Übertragung personenbezogener Daten erfolgt ausschließlich im Rahmen des Bestellprozesses, dem Abruf von Kundendaten im Servicefall, innerhalb des Mahnverfahrens, zur Registrierung von Domains und SSL Zertifikaten, und zur Datensicherung der Kundenumgebungen.
- Erhebt, verarbeitet oder nutzt ein Kunde im Rahmen des Hostingvertrages personenbezogene Daten, so obliegt die Absicherung der Datenübertragung (z.B. über HTTPS) seiner Verantwortung.
- Nicht mehr benötigte oder defekte Datenträger werden durch ein zertifiziertes Unternehmen entsorgt.

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Es gibt je nach gewähltem Hostingmodell mindestens eine logische (virtuelle) Mandantentrennung.
- Es obliegt der Verantwortung des Kunden innerhalb seiner Kundenumgebung sicher zu stellen, dass dieses in gleichem Maß für von Ihm erhobene personenbezogene Daten gilt.

1.6 Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- Die Pseudonymisierung personenbezogener Daten im Rahmen des Hostingvertrages und der dort

vom Auftraggeber betriebenen Anwendungen obliegt dem Auftraggeber.

1.7 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

- Verschlüsselte Datenübertragung (verschlüsselte Internetverbindungen mittels TLS/SSL).

2. Integrität

2.1 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Die Eingabe, Änderung oder Löschung personenbezogener Daten, die im Verantwortungsbe-reich der Mittwald CM Service GmbH & Co KG liegen, werden mit der Kennung des zuständigen Mitarbeiters geloggt.

- Erhebt, verarbeitet oder nutzt ein Kunde im Rahmen des Hostingvertrages personenbezogene Daten, so obliegt es seiner Verantwortung entsprechende Loggingmechanismen für seine Webumgebung zu implementieren.

2.2 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem 1.4 dienen auch der Sicherstellung der Integrität.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Soweit es technisch möglich ist, sind sämtliche auf Datenverarbeitungssystemen der Mittwald CM Service GmbH & Co KG liegenden Daten im Rahmen der Ausfallsicherheit vor zufälligem Verlust oder Zerstörung geschützt.

- Hierzu kommen u.a. RAID Systeme, Ersatzhardware, Überspannungsschutz, USV-Anlagen, Notstromaggregat, Löschgasanlage zum Einsatz.

- Weitergehend wird mindestens ein Backup des Vortages (tarifabhängig) bereitgehalten.

- Beim Produkt Root-Server findet keinerlei Backup statt, der Auftraggeber muss selbst für eine geeignete Datensicherung sorgen.

3.2 Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

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

4. Weitere Maßnahmenbereiche

4.1 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Managementsystem zum Datenschutz und der Informationssicherheit.
- Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen.
- Durchführung regelmäßiger IT-Schwachstellenanalysen.
- Durchführung regelmäßiger interner Audits.
- Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen.

4.2 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

- Personenbezogene Daten werden von der Mittwald CM Service GmbH & Co KG nur im Rahmen des Bestellprozesses, sowie bei Logging von Verbindungsdaten (IP-Adressen) erhoben, verarbeitet und genutzt.
- Von Kunden erhobene personenbezogene Daten werden ausschließlich im Servicefall im Auftrag des Kunden verarbeitet (Erstellung und Wiederherstellung eines Backups, Reparatur der Kundendatenbank, o.ä.).
- Für den Umgang mit Kundendaten werden nur die unter https://www.mittwald.de/unsere-dienstleister genannten Unterauftragnehmer als externe Dienstleister eingesetzt.

Anlage 3
Weitere Auftragsverarbeiter

Gemäß § 7.1 stimmt der Auftraggeber mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgende weitere Auftragsverarbeiter im Rahmen der Datenverarbeitungstätigkeiten einsetzt:

Unterauftragnehmer	**Region**	**Leistungsbeschreibung**	**Angemessenes Schutzniveau**
Mittwald CM Service GmbH & Co. KG Königsberger Straße 4-6 32339 Espelkamp	EU/EWR (DE)	Rechenzentrum Webhoster Serverbetreiber Email-Versand Email-Hosting	
ALL-INKL.COM - Neue Medien Münnich Hauptstraße 68 02742 Friedersdorf	EU/EWR (DE)	Rechenzentrum Webhoster Serverbetreiber Email-Versand Email-Hosting	
PayPal (Europe) S.à r.l. et Cie, S.C.A. 22-24 Boulevard Royal L-2449 Luxembourg	EU/EWR (LUX)	Technischer Dienstleister im Bereich Zahlungsabwicklung Payment Service Provider	
Klarna Bank AB (publ) Sveavägen 46 111 34 Stockholm Schweden	EU/EWR (SWE)	Technischer Dienstleister im Bereich Zahlungsabwicklung Payment Service Provider	
Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043,USA	Drittstaat (US)	Webanalyse Email-Versand Email-Hosting Technischer Dienstleister im Bereich Cloudspeicher	EU-US Privacy Shield Framework
Collmex GmbH Lilienstraße 37 66119 Saarbrücken	EU/EWR (DE)	Finanzbuchhaltung	
Pipedrive Paldiski mnt 80 Tallinn 10617 Estonia	EU/EWR (EST)	CRM SaaS oder Cloud basierende Angebote der Software Überlassung	
INWX GmbH & Co. KG Prinzessinenstr. 30 10969 Berlin	EU/EWR (DE)	Rechenzentrum Webhoster Serverbetreiber Email-Versand Email-Hosting	