Datenschutzvereinbarung zu Software as a Service (SaaS) im Auftrag

gemäß Art. 28 DS-GVO

mit der

Mittwald CM Service GmbH & Co. KG
Königsberger Straße 4-6
32339 Espelkamp

(nachstehend Auftragnehmer genannt)

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in dieser Vereinbarung und der in Anlage A beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Dienstleistung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.
Den Parteien ist bekannt, dass seit dem 25.05.2018 die EU Datenschutz-Grundverordnung (DS-GVO: EU-Verordnung 2016/679) gilt und sich die Vorgaben der Auftragsverarbeitung grundsätzlich nach Art. 28 DS-GVO richten. Diese Vereinbarung ersetzt frühere Vereinbarungen zum Datenschutz gem. § 11 BDSG.
Einzelvereinbarungen in dieser Datenschutzvereinbarung gehen den Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers vor.

§ 1 Definitionen

1. **Personenbezogene Daten**
   Nach Art. 4 Abs. 1 DS-GVO sind 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2. **Auftragsverarbeiter**
   Nach Art. 4 Abs. 8 DS-GVO ist ein Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

3. **Weisung**
   Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Speicherung, Pseudonymisierung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete, in der Regel schriftliche Anordnung des Auftraggebers. Die Weisungen werden vom Auftraggeber erteilt und können durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer erbringt im Auftrag des Auftraggebers SaaS-Leistungen. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogenen Daten bekommt bzw. Kenntnis von diesen erlangt. Nach Art 28 DS-GVO ist daher der Abschluss einer Vereinbarung zur Verarbeitung im Auftrag erforderlich.

2. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DS-GVO als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich bzw. auch elektronisch erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den Auftrag zur Auftragsverarbeitung i.S.d. Art 28 Abs. 3 DS-GVO und regelt die Rechte und Pflichten der Parteien zum Datenschutz im Zusammenhang mit der Erbringung von SaaS-Leistungen.

3. Das Eigentum an den personenbezogenen Daten liegt ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.

§ 3 Gegenstand und Dauer des Auftrages

1. Der Gegenstand des Auftrages ist in Anlage A niedergelegt.

2. Diese Vereinbarung beginnt mit dem Abschluss durch den Auftraggeber und endet mit Kündigung des Hauptvertrages. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

§ 4 Beschreibung der Verarbeitung, Daten und betroffener Personen

Umfang, Art und Zweck der Verarbeitung sind ebenso wie die Art der Daten und der Kreis der betroffenen Personen in Anlage A beschrieben.

§ 5 Technische und organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Wahrung der anzuwendenden Datenschutzvorschriften angemessen und erforderlich sind.

1. Da der Auftragnehmer die SaaS-Leistungen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt, sind vom Auftragnehmer zwingend die von ihm getroffenen technischen und organisatorischen Maßnahmen i.S.d. Art. 28 Abs. 3 lit. C DS-GVO, Art. 32 DS-GVO i.V.m. Art. 5 Abs. 1 und Abs. 2 DS-GVO hierzu zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.
2. Die Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der mit diesem Auftrag in Zusammenhang stehenden 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.
3. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage B „Technische und organisatorische Maßnahmen zum Datenschutz“ dieser Vereinbarung beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

§ 6 Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber zur Erledigung durch diesen weiterleiten.
2. Die Umsetzung der Rechte auf Löschung, Berichtigung, Datenübertragbarkeit und Auskunft sind nur nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.
3. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten oder aufgrund gerichtlicher oder behördlicher Anordnung erforderlich sind.

4. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer dem Auftraggeber die Möglichkeit zum Zugriff und zur Sicherung sämtlicher in seinen Besitz gelangter Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, einzuräumen und diese nach Aufforderung unter Einhaltung datenschutzrechtlicher Bestimmungen zu löschen bzw. zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

5. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 7 Pflichten des Auftragnehmers

1. Eine Verarbeitung personenbezogener Daten, die sich nicht auf die Erbringung von SaaS-Leistungen bezieht, ist dem Auftragnehmer untersagt. Es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat, z.B. auch im Rahmen eines weiteren Hauptvertrages oder einer weiteren Vereinbarung zur Auftragsverarbeitung.

2. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörde); 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 Interesse verbietet (Art. 28 Abs. 3 Satz 2lit. A DS-GVO).

3. Der Auftragnehmer bestätigt, dass er – soweit dieser gesetzlich dazu verpflichtet ist – einen betrieblichen Datenschutzbeauftragten i.S.d. Artt. 38, 39 DS-GVO bestellt hat. Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt:
   Herr Andreas Durnio, datenschutz@mittwald.de
   Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

4. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Auftraggebers.

6. Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten einer Verletzung des gesetzlichen Schutzes personenbezogener Daten gem. Art. 33 DS-GVO (Datenschutzverstoß bzw. Datenpanne) unterliegen, z.B. indem diese unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls bzw. der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Meldung an den Auf-traggeber muss mindestens folgende Informationen enthalten:
   a. Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze.
   b. Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen.
   c. Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.
   d. Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

7. Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO notwendigen Angaben zur Verfügung und führt als Auftragsverarbeiter selbst ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO.

8. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO zur Wahrung der Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugriff auf personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.

9. Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.
10. Des Weiteren verpflichtet sich der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DS-GVO bei der Einhaltung der in Artt. 32 - 36 DS-GVO genannten Pflichten zu unterstützen:
    a. Im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen und dem Auftraggeber in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
    b. Bei der Durchführung seiner Datenschutz-Folgenabschätzung.
    c. Im Rahmen einer vorherigen Konsultation mit der Aufsichtsbehörde.
11. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

12. Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt. Eine Information erfolgt nicht, soweit dies gerichtlich oder behördlich untersagt ist.

13. Soweit der Auftraggeber 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 durch den Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

14. Der Auftragnehmer 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 des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

§ 8 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Entwicklung, Pflege und Wartung von Software und/oder IT-Systemen gegenüber dem Auftragnehmer zu erteilen. Weisungen können
   a. schriftlich
   b. per Fax
   c. per E-Mail
   d. mündlich

   erfolgen. Der Auftraggeber soll mündliche Weisungen unverzüglich in Textform (z.B. Fax oder E-Mail) gegenüber dem Auftragnehmer bestätigen.

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

3. Dem Auftraggeber obliegen die aus Art. 33 Abs. 1 DS-GVO resultierenden Meldepflichten.

4. Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten personenbezogenen Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

5. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen und nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, sind die dadurch begründeten und nachgewiesenen tatsächlichen Kosten vom Auftraggeber zu tragen. Der Auftragnehmer hat den Auftraggeber vor Umsetzung der diesbezüglichen Einzelweisung darüber zu informieren, dass diese mit Zusatzkosten (Art und Höhe) verbunden sein wird. Erst ein nach Informationszugang erteilter Auftrag ist verbindlich.

§ 9 Wahrung von Rechten der betroffenen Person

1. Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person verantwortlich.

2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

3. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Einschränkung oder Datenübertragbarkeit seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

§ 10 Kontrollbefugnisse

1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Abs. 1 erforderlich ist.

3. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Abs. 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

4. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DS-GVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

5. Der Auftragnehmer erbringt den Nachweis technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen. Dabei kann dies erfolgen durch:
   a. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.
   b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO.
   c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Datenschutzauditoren.
   d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder BSI-Grundschutz).

6. Die Kosten für Aufwände einer Kontrolle beim Auftragnehmer gem. Abs. 3 und 4 können gegenüber dem Auftraggeber geltend gemacht werden. Ein individuelles Angebot kann jederzeit eingeholt werden.

§ 11 Unterauftragsverhältnisse

1. Der Auftragnehmer nimmt für die Erbringung von SaaS-Leistungen im Auftrag des Auftraggebers nur Leistungen von den jeweils unter www.mittwald.de/unsere-dienstleister genannten Dritten in Anspruch, die in seinem Auftrag Daten gem. Art. 28 DS-GVO verarbeiten („Unterauftragnehmer“). Der Auftragnehmer hält diese Liste fortwährend auf dem aktuellen Stand.

2. Zum Zeitpunkt des Abschlusses dieses Vertrages werden die folgenden Unterauftragnehmer vom Auftragnehmer eingesetzt, mit denen sich der Auftraggeber einverstanden erklärt:
   weißaufschwarz GmbH, Königsberger Str. 4-6, 32339 Espelkamp (Betrieb der Software)
   Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung weiterer oder die Ersetzung bestehender Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrechtlichen Grund innerhalb einer Frist von 14 Tagen nach Zugang der Information über die Ände-rung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist nach Zugang des Einspruchs einstellen. Unterbleibt der Einspruch des Auftraggebers, erkennt dieser damit den oder die neuen Unterauftragnehmer an.

3. Im Falle einer Beauftragung hat der Auftragnehmer den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf

Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. Artt. 37-39 DS-GVO bestellt hat.

4. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.
5. Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen, sofern keine andere Form angemessen ist. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

6. Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 10 dieser Vereinbarung) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

§ 12 Datengeheimnis und Geheimhaltungspflichten

1. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist.

3. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieser Vereinbarung erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den oben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

4. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 13 Haftung

Es wird auf die Haftungsregelungen des Art. 82 DS-GVO verwiesen.

§ 14 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die personenbezogenen 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 personenbezogenen Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO liegen.

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. Bei Unwirksamkeit einer Bestimmung in diesen Vertragsbedingungen bleiben die übrigen Bestimmungen gleichwohl wirksam. Die Vertragsparteien verpflichten sich, eine unwirksame Bestimmung oder eine planwidrig fehlende Bestimmung nach Treu und Glauben durch eine Bestimmung zu ersetzen, die dem gemeinsam verfolgten Zweck der Vertragsparteien am nächsten kommt.

Anlage A: Details zum Auftrag

1. **Gegenstand des Auftrages**
   Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:
   Zeitlich beschränkte entgeltliche Bereitstellung von Standardsoftware zur Nutzung ihrer Funktionalitäten sowie, soweit vereinbart, die Bereitstellung von Speicherplatz (Software as a Service (SaaS)). Einzelheiten sind in der Leistungsbeschreibung des Hauptvertrages geregelt.

2. **Umfang, Art und Zweck der Verarbeitung**
   Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DS-GVO verarbeitet.
   Zweck der Verarbeitung ist das Bereitstellen der Standardsoftware, der dafür notwendigen Infrastruktur und ggfls. das Hosting.
   Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Vertrages.
   Die Erbringung der vertraglich vereinbarten Datenverarbeitung kann auch außerhalb der Mitgliedsstaaten der Europäischen Union und in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden.

3. **Art der Daten**
   - Nutzungsdaten (Protokollierung der Nutzeraktivitäten, Log-Files, IP-Adressen)
   - Kundendaten (Anschriften, Kontaktdaten, Bestelldaten, Umsätze, Kontodaten)
   - Beschäftigtendaten (Fotos, Namen, Kontaktdaten, Geburtsdaten, Personaldaten, Kontodaten)
   - Vertragsdaten
   - Beteiligungsdaten
   - Steuerdaten
   - E-Mails
   - Daten aus Online-Umfragen
   - PDF-Downloads

4. **Kategorien der betroffenen Personen**
   - Beschäftigte und ehemalige Beschäftigte des Auftraggebers
   - Webseitenbesucher
   - Kunden und Interessenten des Auftraggebers
   - Lieferanten
   - Ansprechpartner
   - Interessenten
   - Handelspartner
   - Abonnenten/ Mitglieder
   - Bevollmächtigte
   - E-Mail-Kontakte
   - Schüler/ Teilnehmer
   - Bewerber

Anlage B: Technische und organisatorische Maßnahmen zum Datenschutz

gemäß Artt. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO

1. Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der SaaS-Leistung genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

- 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 verwehrt.
- 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 in der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

- 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- 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 SaaS-Vertrages 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Es gibt 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Die Pseudonymisierung personenbezogener Daten im Rahmen des Saas-Vertrages 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.

Durch den Auftragnehmer umgesetzte Maßnahmen:

- 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Die Eingabe, Änderung oder Löschung personenbezogener Daten, die im Verantwortungsbereich 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 SaaS-Vertrages 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- 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.

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.

Durch den Auftragsnehmer umgesetzte Maßnahmen:

- IT-Notfallpläne und Wiederanlaufpläne
- Regelmäßige und dokumentierte Datenwiederherstellungen

4. Weitere Maßnahmenbereiche

4.1 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- 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 Auftragskontrolle

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

Beim Auftragnehmer umgesetzte Maßnahmen:

- 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 www.mittwald.de/unsere-dienstleister genannten Unterauftragnehmer als externe Dienstleister eingesetzt.