

# **Allgemeine Geschäftsbedingungen (AGB) und Vereinbarung zur Datenverarbeitung zur Teilnahme an „mhi regio“**

## **1. Präambel**

**1.1** Die Märklin-Händler-Initiative, Stuttgarter Str. 55-57, 73033 Göppingen, (nachfolgend „mhi“ oder „Auftragnehmer“) hat eine webbasierte Softwarelösung zur Unterstützung teilnehmender mhi-Händler (nachfolgend „Händler“ oder „Auftraggeber“) entwickelt („Software“). Für die Nutzung der Software und die Erbringung ergänzender Dienstleistungen („Services“) gelten diese Allgemeinen Geschäftsbedingungen („AGB“).

**1.2** Unsere Angebote richten sich nur an Unternehmer (iSd. § 14 BGB), also an natürliche oder juristische Personen oder rechtsfähige Personengesellschaften, die bei Abschluss eines Rechtsgeschäfts in Ausübung ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handeln. Wir schließen keine Verträge mit Verbrauchern (iSd. § 13 BGB).

## **2. Nutzungsrechte**

**2.1** Der Auftragnehmer gewährt dem Auftraggeber für die Laufzeit des Vertrages unter der aufschiebenden Bedingung der vollständigen Zahlung der vereinbarten Vergütung das entgeltliche, weltweite, nicht ausschließliche und nicht übertragbare Recht, die Software bestimmungsgemäß zu nutzen. Der Auftraggeber darf die Software nur im Rahmen der vertraglichen Bestimmungen nutzen. Der Auftraggeber erhält kein Recht am Quellcode der Software. Der Auftraggeber darf die Software nur für eigene Zwecke nutzen. Die Nutzung für eigene Zwecke umfasst dabei die bestimmungsgemäße Nutzung der Produkte für allgemeine Geschäftszwecke des Auftraggebers und die Verarbeitung der Daten des Auftraggebers. Nicht umfasst ist die Nutzung der Produkte für Dritte, beispielsweise als Dienstleister oder eine sonstige Überlassung oder Nutzungsvermittlung an Dritte.

**2.2** Der Auftraggeber ist berechtigt, die Software durch eigene Mitarbeiter oder durch Dritte für seine eigenen Zwecke nutzen zu lassen. Der Auftragnehmer kann hierfür einen oder mehrere User für den Auftraggeber anlegen. Der Auftraggeber ist verantwortlich für die Nutzung der Software durch seine User und sämtliche Schäden, die durch fahrlässige oder vorsätzliche Pflichtverletzungen seiner User verursacht wurden.

**2.3** Der Auftraggeber erhält kein Recht am Quellcode der Software.

**2.4** Soweit nicht anders vereinbart, stehen sämtliche Rechte an Software und Services, welche durch den Auftragnehmer bereitgestellt oder unter diesem Vertrag entwickelt werden, einzig dem Auftragnehmer zu. Sämtliche Rechte an jeder Art von Veränderung, Entwicklung oder Verbesserung der Produkte oder Dienstleistungen, welche durch den Auftraggeber vorgenommen werden, stehen ebenfalls ausschließlich dem Auftragnehmer zu.

**2.5** Die Software kann Open Source Software-Komponenten enthalten. Die Nutzung dieser Komponenten unterliegt ausschließlich den entsprechenden Nutzungsbedingungen der Open Source Software-Komponenten, die im Rahmen der Open Source Software-Komponenten übermittelt und/oder referenziert werden. Keine Vorschrift dieser AGB beeinflusst dabei die Rechte oder Pflichten des Auftraggebers aus den entsprechenden

Nutzungsbedingungen der Open Source Software-Komponenten. Im Falle von Widersprüchen oder entgegenstehenden Vorschriften von Lizenzbestimmungen der Open Source Software und den Bestimmungen dieser AGB genießen die Lizenzbestimmungen der Open Source Software Vorrang.

**2.6** Das Nutzungsrecht an der Software erstreckt sich auch auf Fixes, Patches, Entwicklungen und Updates, welche der Auftragnehmer dem Auftraggeber zur Verfügung stellt. Das Recht auf Updates beinhaltet nicht das Recht auf ein Nutzungsrecht an neuen/zusätzlichen Produkten und Funktionalitäten, die als separates Produkt/Modul zur Verfügung gestellt werden.

- 2.7** Soweit nicht anders vereinbart oder aufgrund zwingenden Rechts oder anwendbarer Open Source Software-Nutzungsbedingungen vorgeschrieben, ist der Auftraggeber nicht berechtigt,
- a) die Software über das für die vertragsgemäße Nutzung erforderliche hinausgehende Maß zu kopieren, weder im Ganzen noch teilweise;
  - b) die Software zu modifizieren, zu korrigieren, anzupassen, zu übersetzen, zu verbessern oder sonst abgeleitete Entwicklungen an der Software vorzunehmen;
  - c) die Software zu vermieten, zu verleihen, zu verkaufen, zu lizenzieren, zu übertragen oder sonst Dritten zugänglich zu machen;
  - d) die Software zurückzuentwickeln, zu dekompileieren, zu disassemblieren oder auf andere Weise zu versuchen, den Quellcode der Software zu entschlüsseln, weder im Ganzen, noch teilweise;
  - e) Sicherheitseinrichtungen oder Schutzmechanismen, welche in der Software enthalten oder für sie genutzt werden, zu umgehen oder zu verletzen;
  - f) Maßnahmen zu ergreifen, die geeignet sind, Schaden an der Software oder den Servern des Auftragnehmers hervorzurufen;
  - g) Marken, Dokumentation, Garantien, Haftungsausschlüsse oder sonstige Rechte, wie etwa geistiges Eigentum, Zeichen, Mitteilungen, Markierungen oder Seriennummern, welche in Verbindung zur Software oder Dokumentation stehen, zu entfernen, zu löschen, zu tilgen, zu verändern, zu verdecken, zu übersetzen, zu kombinieren, zu ergänzen oder auf andere Weise abzuändern;
  - a. die Software in einer Art und Weise zu nutzen, durch die geltendes Recht und/oder die Rechte Dritter verletzt werden;
  - h) die Software für Zwecke des Benchmarkings bzw. der Wettbewerbsanalyse der Software, für die Entwicklung, Verwendung oder die Bereitstellung eines konkurrierenden Software-Produkts bzw. konkurrierender Services oder zu sonst einem Zweck zu nutzen, welcher dem Auftragnehmer zum Nachteil gereicht; und/oder
  - i) die Software für oder in Zusammenhang mit der Planung, der Konstruktion, der Instandhaltung, dem Betrieb oder der Nutzung von gefährlichen Umgebungen, Systemen oder Anwendungen oder anderen sicherheitskritischen Anwendungen zu nutzen oder sonst die Software in einer Weise einzusetzen, bei der die Software zu körperlichen Schäden oder schweren Sachschäden führen könnte.

### **3. Verpflichtungen des Auftraggebers**

**3.1** Der Auftraggeber wird den Auftragnehmer bei der Erbringung der vertragsgegenständlichen Leistungen in angemessenem Umfang unterstützen. Der Auftraggeber hat unaufgefordert sämtliche Mitwirkungsleistungen, Informationen, Daten, Dateien, Materialien, welche für die Erfüllung der Vertragspflichten durch den Auftragnehmer erforderlich sind (beispielsweise händlerspezifischen Daten „Über uns“, Kontaktdaten, Öffnungszeiten etc.), im Voraus zur Verfügung zu stellen. Sollte der Auftraggeber nicht ausreichend kooperieren und/oder Verzögerung verursachen, ist der Auftragnehmer nicht verpflichtet, die vertraglichen Verpflichtungen zu erfüllen, so lange und so weit, wie der Auftragnehmer an der Erfüllung der vertraglichen Verpflichtungen aufgrund unzureichender und/oder verspäteter Mitwirkung des Auftraggebers gehindert ist. Der Auftragnehmer hat den Auftraggeber über seine nicht ausreichende oder rechtzeitige Zusammenarbeit zu informieren und eine angemessene Frist zur Nacherfüllung zu setzen. Erfüllt der Auftraggeber dennoch seine Mitwirkungspflichten nicht, so gehen etwaige für den Auftragnehmer nicht vermeidbare sich daraus ergebenden Vergütungserhöhungen, zusätzliche Aufwände (z.B. Mehrarbeit, Stornokosten, Reisekosten) und Terminverschiebungen zu seinen Lasten. Nach fruchtlosem Ablauf der Nachfrist gelten die betroffene Software

bzw. der betroffene Service als zur Verfügung gestellt bzw. erbracht.

**3.2** Der Auftraggeber ist verantwortlich für (i) angemessene Sicherheitsprozesse, Tools und Steuerungen für Systeme und Netzwerke, welche mit der Software interagieren, (ii) das Vorhalten alternativer Prozesse im Falle einer mangelnden Verfügbarkeit der Software, (iii) die Feststellung, ob die vom Auftragnehmer zur Verfügung gestellten technischen und organisatorischen Maßnahmen des Datenschutzes und der Datensicherheit den spezifischen Anforderungen des Auftraggebers genügen; (iv) das angemessene interne Training der User und die Bereitstellung von internem technischen Support; und (v) die ordnungsgemäße Sicherung sämtlicher auf seiner Systemumgebung befindlichen Programme und Daten und sämtlicher in die Software übertragener bzw. mit der Software erstellter Daten und Arbeitsergebnisse mit Beginn der Nutzung der Software und anschließend in angemessenen regelmäßigen Abständen.

## **4 Gewährleistung**

**4.1** Die Software wird vom Auftragnehmer mangelfrei zur Verfügung gestellt bzw. erbracht und entspricht bei bestimmungsgemäßer Nutzung im Wesentlichen den in der Produktbeschreibung genannten Spezifikationen.

**4.2** Der Einräumung der vereinbarten Nutzungsrechte an den Auftraggeber stehen keine geistigen Eigentumsrechte Dritter entgegen.

**4.3** Technische Daten, Spezifikationen und Leistungsangaben in öffentlichen Äußerungen, insbesondere in Werbemitteln, sind keine Beschaffenheitsangaben.

**4.4** Im Fall der Mangelhaftigkeit sind die Mängelansprüche des Auftraggebers zunächst auf Nacherfüllung beschränkt. Der Auftraggeber wird dem Auftragnehmer auftretende Mängel schriftlich mit Beschreibung des Mangels mitteilen und zur Mängelbeseitigung auffordern. Der Auftragnehmer leistet bei nachgewiesenen Mängeln Gewähr durch Nacherfüllung in der Weise, dass der Auftragnehmer die Software erneut in mangelfreiem Zustand zur Verfügung stellt bzw. erbringt oder den Mangel beseitigt.

**4.5** Falls die Nacherfüllung nach zwei Nacherfüllungsversuchen endgültig fehlschlägt, kann der Auftraggeber vom jeweiligen Einzelvertrag zurücktreten oder die Vergütung angemessen mindern. Schadensersatz oder Ersatz vergeblicher Aufwendungen wegen eines Mangels leistet der Auftragnehmer im Rahmen der in diesen AGB festgelegten Grenzen der Haftung.

## **5 Zurverfügungstellung der Software und Erbringung der Services**

**5.1** Die Software wird als „Software as a Service (SaaS)“ zur Verfügung gestellt, das heißt der Auftragnehmer stellt die Software für den Auftraggeber in einem logisch separierten Account zum Fernzugriff über das Internet zur Verfügung. Eine Überlassung oder Weitergabe der Software an den Auftraggeber findet nicht statt. Die Software wird dem Auftraggeber in ihrer jeweils aktuellen Version/Release zur Verfügung gestellt.

**5.2** Der Auftragnehmer wird dem Auftraggeber die Software mit einer Verfügbarkeit von mindestens 99,5 % über ein Quartal zur Verfügung stellen (nachfolgend „Mindestverfügbarkeit“). Verfügbar ist die Software in diesem Zusammenhang, wenn zwischen den Servern, auf denen die Software gehostet wird, und dem Übergabepunkt zum Internet eine ununterbrochene Verbindung besteht und der Auftraggeber in der Lage ist, sich anzumelden und Zugriff auf die Software hat. Die Mindestverfügbarkeit bezieht sich nicht auf Test- und Entwicklungsserver.

**5.3** Auf Basis der mit der Software erhobenen und analysierten Daten generiert die Software im Rahmen bestimmter Anwendungsfälle Auswertungen, Reports, und Analysen.

**5.4** Für die Nutzung der Software benötigt der Auftraggeber einen aktuellen Standardwebbrowser (z.B. Google Chrome oder Mozilla Firefox). Der Auftraggeber ist für die Bereitstellung und den Betrieb sämtlicher Hardware und Betriebssoftware sowie für eine sichere und schnelle Internetverbindung verantwortlich.

**5.5** Soweit nicht ausdrücklich anders vereinbart, sind Setup/Einrichtung und Konfiguration der Software gemäß der im jeweiligen Einzelauftrag anfallenden Einrichtungsgebühr enthalten.

**5.6** Software und sonstige Arbeitsergebnisse gelten als übergeben, sobald sie dem Auftraggeber zur Verfügung gestellt wurden. Services gelten als erbracht, sobald der jeweilige Service abgeschlossen wurde. Support/Pflege wird gegebenenfalls mit Zeitablauf als monatlich anteilig erbracht angesehen.

**5.7** Sofern nicht anders vereinbart, unterliegen Software und Services keiner gesonderten Abnahme durch den Auftraggeber, sondern gelten mit Übergabe als abgenommen. Sollte eine Abnahme vertraglich vereinbart sein und hat der Auftraggeber nicht den Zeit- oder Testplan der Abnahme eingehalten oder sollte ein solcher Testplan oder eine zeitliche Begrenzung für Tests und Abnahme nicht vorliegen, so gelten Software und Services zehn Werktage nach Übergabe als abgenommen.

**5.8** Der Auftragnehmer ist berechtigt, Subunternehmer oder sonstige Erfüllungsgehilfen (insgesamt als „Subunternehmer“ bezeichnet) einzusetzen, um die vertraglichen Verpflichtungen zu erfüllen.

Der Auftragnehmer wird dafür sorgen, dass Subunternehmer entsprechend dieser AGB an Verpflichtungen hinsichtlich Geheimhaltung und Datenschutz gebunden sind. Die Beauftragung von Subunternehmern lässt die vertraglichen Verpflichtungen des Auftragnehmers dem Auftraggeber gegenüber unberührt. Der Auftragnehmer haftet für eventuelle Schlechtleistungen eines Subunternehmers wie für eigenes Verschulden.

**5.9** Bei Nutzung der Shop-Funktion werden alle vom Auftragnehmer bereitgestellten Produkte im Online-Shop des Auftraggebers angezeigt; eine Ausblendung einzelner Artikel durch den Auftragnehmer ist nicht vorgesehen. Führt der Auftragnehmer bestimmte Produkte nicht oder hat diese vorübergehend nicht vorrätig, werden sie im Shop als nicht verfügbar bzw. ausverkauft gekennzeichnet. Eine Einschränkung der Shop-Funktion auf bestimmte Warengruppen oder eine Teilnutzung (etwa nur Online-Shop oder nur Marktplatz) ist technisch und vertraglich ausgeschlossen.

**5.10** Der mhi-Shop kann nur in Verbindung mit dem mhi-Regio Webseiten-Tool betrieben werden. Eine Nutzung des mhi-Shop oder des Marktplatzes ohne eine aktive mhi regio Website des Händlers ist ausgeschlossen.

**5.11** Die Entscheidung über die Freischaltung der Shop-Funktion für einen jeweiligen Händler liegt im Ermessen von mhi. mhi behält sich vor, eine Freischaltung im Einzelfall abzulehnen.

**5.12** Bei Verstößen des Händlers gegen die AGB oder anderen Verträgen zu mhi ist mhi berechtigt, die Shop-Funktion für den betreffenden Händler vorübergehend oder dauerhaft zu sperren. Unabhängig davon kann mhi einen Händler ganz von der Nutzung der Shop-Plattform ausschließen., insbesondere wenn der Händler wiederholt negative Kundenerfahrungen verursacht, seine Pflichten nachhaltig verletzt oder die qualitativen Anforderungen von mhi an den Online-Verkauf nicht erfüllt.

## **6 Pflichten bei der Nutzung von mhi regio website und mhi regio newsletter**

**6.1** Der Auftraggeber ist Dienstanbieter der Internetseite und der von ihm versandten E-Mails und als solcher Verantwortlicher. Damit ist er verpflichtet, auf der Webseite und in Newslettern rechtliche Angaben vorzuhalten und einzuhalten, insbesondere

- ein vollständiges Impressum vorzuhalten, welches unter anderem folgende Angaben enthält: (so vorhanden) Firmenname, Rechtsform, Vertretungsberechtigte, vollständiger Anschrift und E-Mail-Adresse
- eine Datenschutzerklärung nach der Datenschutz-Grundverordnung (DS-GVO), in welcher über die Datenverarbeitungsvorgänge aufgeklärt wird,
- ggf. eine Barrierefreiheitserklärung.

Der Auftragnehmer stellt dem Auftraggeber hierfür Muster zur Verfügung. Diese Muster sind unverbindlich und stellen keine Rechtsberatung im Einzelfall dar. Der Auftragnehmer übernimmt keine Garantenstellung gegenüber dem Auftraggeber. Der Auftraggeber ist verpflichtet, diese Muster ggf. anzupassen oder zu ersetzen.

**6.2** Die für den Auftraggeber individualisierte Plattform wird unter der Domain <https://Händlername-Händlerort.mhi.de> aufgesetzt. Eigentümer der Domain ist der Auftragnehmer. Ein Anspruch auf Erwerb der Domain durch den Auftraggeber besteht nicht.

**6.3** Der Auftraggeber erklärt verbindlich, dass E-Mails ausschließlich an Empfänger des Auftraggebers verschickt werden, die dem Empfang von Werbe-E-Mails vorher nachweisbar zugestimmt haben (z. B. durch das Double-Opt-In Verfahren oder durch schriftliche Vereinbarung).

**6.4** Der Auftraggeber ist verpflichtet, in Opt-In-E-Mails bekannt zu geben, warum der Empfänger das Mailing erhält. In der Kopf- und Betreffzeile der E-Mail darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Der Auftraggeber muss jedem Empfänger die Möglichkeit einräumen, sich aus der E-Mail heraus wieder aus der Datenbank austragen zu können. Darauf hat der Auftraggeber in jeder E-Mail ausdrücklich hinzuweisen.

**6.5** Dem Auftraggeber ist bekannt, dass die Versendung von Mailings ins Ausland den Rechtsordnungen der jeweiligen Empfängerstaaten unterliegen können und verpflichtet sich, die in diesen Staaten geltenden Gesetze oder sonstigen Vorschriften im Hinblick auf die versendeten Mailings einzuhalten. Er verpflichtet sich, mit mhi Newsletter keine Mailings zu verschicken, deren Inhalt in einem Staat, in dem der Empfänger seinen Aufenthaltsort oder Sitz hat, gesetzlichen Verboten unterliegt.

**6.6** Der Auftraggeber ist bei der Verwendung von E-Mail-Adressen, die er von Dritten erworben hat, verpflichtet, sich vor der Vornahme des Newsletterversandes zu vergewissern, dass tatsächlich nur solche Empfänger angeschrieben werden, die eine Einwilligung hierin erklärt haben, die sich nicht nur auf den Versand durch einen Dritten, sondern auch durch den Versender bzw. seinen Kunden selbst bezieht. Insbesondere dürfen so gewonnene Adressdaten für eine Versendung nur genutzt werden, wenn bei Erhebung die Unternehmen, Verbände etc., für die die Adressdaten generiert wurden, transparent, namentlich und unter Angabe der Branche einzeln benannt wurden, sowie die Kenntnisnahme der Liste der Unternehmen für den Empfänger leicht, und eindeutig möglich war und die Anzahl der Unternehmen bzw. Personen, für die die Adressdaten erhoben wurden, auf ein Maß reduziert ist, das die Weiterleitung der Nutzerdaten an einen unverhältnismäßig großen Kreis Dritter ausschließt und dem Nutzer erlaubt, die Tragweite und den Umfang seiner Einwilligung einfach zu erfassen sowie den rechtlichen Umgang mit seinen Daten einfach zu kontrollieren. Die Gewinnung von Adressdaten für Dritte (etwa durch Co-Sponsoring) muss gegenüber dem Nutzer transparent sein.

**6.7** Die Nutzung des mhi Newsletter mit nachweislich unseriösen Geschäftspraktiken ist untersagt. Unseriös sind insbesondere E-Mails, deren Inhalt grob anstößig ist oder gegen gesetzliche Verbote verstößt oder unzulässig sind, wie beispielsweise (i) E-Mails, deren Inhalt gegen gesetzliche Bestimmungen der Bundesrepublik Deutschland und/oder europäisches Gemeinschaftsrecht verstoßen; (ii) E-Mails, die Rechte Dritter, wie z. B. gewerbliche Schutzrechte (Marken, Urheberrechte, etc.) oder das allgemeine Persönlichkeitsrecht (einschließlich des Rechts auf informationelle Selbstbestimmung) verletzen; (iii) E-Mails mit pornographischem Inhalt bzw. Verstoß gegen die Bestimmung des Jugendschutzgesetzes; (iv) Mailings, die einen rassistischen, verleumderischen, beleidigenden, Gewalt verherrlichenden, und/oder diskriminierenden Inhalt.



**6.8** mhi behält sich eine stichprobenartige Inhaltsprüfung der über mhi Newsletter versandten Mailings vor.

## **7 Pflichten bei der Nutzung von mhi shop**

**7.1** Der Auftraggeber ist Dienstanbieter des Shops und als solcher Verantwortlicher. Damit ist er verpflichtet, im Shop rechtliche Angaben vorzuhalten und einzuhalten, insbesondere Informationspflichten zum Betreiber, zu Produktsicherheit, zu Widerruf und Rücknahme, Verpackungsmittel, Batterien etc. Der Händler hat alle weiteren einschlägigen gesetzlichen Vorschriften im Zusammenhang mit dem Vertrieb seiner Waren über den Online-Shop einzuhalten, insbesondere solche aus dem Wettbewerbsrecht, Verbraucherrecht, Kaufvertragsrecht sowie Datenschutzrecht.

Der Auftragnehmer stellt dem Auftraggeber hierfür Muster zur Verfügung. Diese Muster sind unverbindlich und stellen keine Rechtsberatung im Einzelfall dar. Der Auftragnehmer übernimmt keine Garantenstellung gegenüber dem Auftraggeber. Der Auftraggeber ist verpflichtet, diese Muster ggf. anzupassen oder zu ersetzen.

**7.2** Die Shop-Funktion ist ausschließlich für Artikel, die von mhi zentral in das System eingespielt werden. Der Händler ist nicht berechtigt, eigenständig Artikel, insbesondere Produkte außerhalb des mhi-Sortiments oder Fremddmarken, in den Shop einzupflegen. mhi behält sich vor, das Sortiment der Shop-Funktion nach eigenem Ermessen zu erweitern, beispielsweise durch die Aufnahme weiterer Marken oder Artikel fremder Hersteller.

**7.3** Der Händler darf über die Shop-Funktion ausschließlich Neuware anbieten.

**7.4** Der Händler ist verpflichtet, die Verfügbarkeiten der Waren sowie Preise korrekt und auf aktuellem Stand im System zu halten.

**7.5** Die vom Händler angegebenen Versandzeiten sind einzuhalten.

**7.6** Der Händler muss über einen aktiven PayPal Business-Account verfügen und die Zahlungsabwicklung über diesen gewährleisten. Stellt mhi weitere Bezahlmethoden als Alternativen im Shop bereit, verpflichtet sich der Händler, deren Abwicklung zu unterstützen (so wird beispielsweise bei Bereitstellung der Bezahlmethode „Vorkasse“ durch mhi der Händler Vorabüberweisungen überprüfen und diese annehmen, bei Bereitstellung von „Zahlung bei Abholung“ wird der Händler vor Ort die Zahlung entgegennehmen).

**7.7** Der Händler verpflichtet sich bei alternativen Lieferoptionen wie „Click & Reserve“ (Online-Reservierung eines Artikels ohne unmittelbaren Kaufabschluss) oder „Click & Collect“ (Online-Bestellung mit anschließender Abholung der Ware im Geschäft) die ordnungsgemäße Bearbeitung der Reservierungen bzw. zur Abholung bestellten Waren durchzuführen, beispielsweise durch Bereitstellung des reservierten Artikels im Laden für Click & Reserve oder Bereithalten der online bestellten Ware für die Abholung bei Click & Collect.

## **8 Zahlungsbedingungen**

**8.1** Soweit nicht anders vereinbart wird die Software jährlich zum Ende der Nutzungsperiode in Rechnung gestellt. Der Auftraggeber hat Rechnungen binnen 30 Tage nach Rechnungsdatum ohne Skonto oder sonstige Abzüge zu zahlen. Bei Zahlungsverzug werden Verzugszinsen in gesetzlicher Höhe fällig. Der Auftragnehmer ist berechtigt, den Zugang des Auftraggebers zur Software bei einem Zahlungsverzug von mehr als 30 Tagen vorübergehend zu deaktivieren, bis die überfällige Rechnung bezahlt wurde. Die angegebenen Preise enthalten keine Umsatzsteuer oder sonstige Steuern. Diese werden dem Auftraggeber gegebenenfalls gesondert in Rechnung gestellt.

**8.2** Die Nutzung der Shop-Funktion erfolgt auf Provisionsbasis und wird monatlich auf Basis der vom Shopanbieter (derzeit e-vendo) bereitgestellten Verkaufszahlen, die als verbindliche Grundlage für die Provisionsabrechnung dient, abgerechnet.

**8.3** Die Provision berechnet sich auf den Brutto-Verkaufspreis exkl. Versandkosten der über die Shop-Funktion verkauften Artikel des Händlers. Für retournierte Waren fällt eine Bearbeitungsgebühr an, deren Höhe sich nach der Retourenquote des Händlers richtet. Die Retourenquote wird ständig rückwirkend für die letzten drei Monate ermittelt und ergibt sich aus dem Verhältnis des Wertes der retournierten Waren zum Gesamtwert der verkauften Waren in diesem Zeitraum. Liegt die Retourenquote über einem festgelegten Schwellwert, fällt eine einfache Bearbeitungsgebühr an; ist die Retourenquote unter dem Schwellwert, fällt eine reduzierte Bearbeitungsgebühr an. Zieht sich die Erstattung des Kaufpreises über eine Abrechnungsperiode, wird in der folgenden Abrechnungsperiode eine entsprechende Gutschrift erstellt.

## **9 Haftungsbegrenzung**

**9.1** Für einfache Fahrlässigkeit haftet der Auftragnehmer, sowohl für eigenes sowie für zugerechnetes Verhalten, nur, sofern wesentliche Vertragspflichten (Kardinalpflichten) verletzt sind. In diesem Fall ist die Haftung begrenzt auf den vertragstypischen und vorhersehbaren Schaden. Wesentliche Vertragspflichten sind solche Pflichten, deren Verletzung die Erreichung des Vertragszwecks gefährdet, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertraut.

**9.2** Für die vorgenannten Fälle begrenzter Haftung wird diese zusätzlich der Höhe nach für jeden Schadensfall auf die Höhe der jährlich vom Auftraggeber zu zahlenden Vergütung (die Vergütung, die in den letzten 12 Monaten vor Schadenseintritt vom Auftraggeber gezahlt wurde bzw. zu zahlen wäre bzw., wenn der Vertrag bei Schadenseintritt noch keine 12 Monate lief, der Durchschnitt der bisherigen Vergütung pro Monat x12) und auf das Doppelte der vom Auftraggeber jährlich zu zahlenden Vergütung für alle sich in einem Vertragsjahr ereignenden Schadensfälle begrenzt.

**9.3** Für mittelbare und Folgeschäden sowie für entgangenen Gewinn, Personalmehrkosten, nutzlose Aufwendungen und unterbliebene Einsparungen etc. haftet der Auftragnehmer nur bei Vorsatz und grober Fahrlässigkeit.

**9.4** Die Haftungsbeschränkungen gelten nicht für Ansprüche wegen Vorsatz und grober Fahrlässigkeit, bei Personenschäden, bei Arglist, soweit das Produkthaftungsgesetz zur Anwendung kommt, sowie für Schäden, die in den Schutzbereich einer vom Auftragnehmer gegebenen eigenständigen Garantie, Beschaffenheits- oder Haltbarkeitsgarantie fallen, sofern sich aus der jeweiligen Garantievereinbarung nicht etwas anderes ergibt.

**9.5** Verletzt der Auftraggeber die ihm obliegende Pflicht zur ordnungsgemäßen Datensicherung, haftet der Auftragnehmer im Rahmen der vorstehenden Bestimmungen bei Verlust von Daten der Höhe nach begrenzt auf diejenigen Schäden, die auch bei ordnungsgemäßer und regelmäßiger Datensicherung durch den Auftraggeber aufgetreten wären.

## **9 Vertraulichkeit**

**9.1** Jede der Parteien verpflichtet sich, alle im Rahmen der vertraglichen Zusammenarbeit erhaltenen Informationen, die (a) als „vertraulich“ oder „geheim“ oder mit einem gleichbedeutenden Hinweis gekennzeichnet sind oder mündlich als vertraulich bezeichnet werden; (b) aufgrund ihres Inhalts als vertraulich anzusehen sind; oder (c) von vertraulichen Informationen, welche zur Verfügung gestellt worden sind, abgeleitet wurden; ausschließlich für die Zwecke der vertraglichen Zusammenarbeit zu verwenden, vertraulich zu behandeln und vor der Kenntnisnahme durch unberechtigte Dritte zu schützen. Diese Vertraulichkeitsverpflichtung ist allen Personen aufzuerlegen, die mit der Durchführung dieses Vertrages betraut werden.

**9.2** Von der Vertraulichkeitsverpflichtung ausgenommen sind Informationen, die (a) öffentlich zugänglich sind oder nachträglich öffentlich zugänglich wurden oder der anderen Partei bei Vertragsschluss bereits bekannt waren; (b) unabhängig und selbstständig von der anderen Partei entwickelt wurden; (c) der anderen Partei von einem Dritten offenbart wurden, der keiner Vertraulichkeitsverpflichtung unterliegt, oder (d) aufgrund gesetzlicher Bestimmungen oder behördlicher oder gerichtlicher Anordnung offengelegt werden müssen (in diesem Falle ist die betroffene Partei hierüber unverzüglich zu unterrichten).

## **10 Datenschutz und Informationssicherheit**

**10.1** Der Auftragnehmer verarbeitet personenbezogene Daten, die im Zusammenhang mit der Einrichtung eines Kontos in Bezug auf die Benutzer der Software zur Verfügung gestellt werden (Name, Vorname, E-Mail-Adresse, Telefonnummer, Passwort) und persönliche Daten, die sich auf die Nutzung der Software beziehen (Log-Dateien). Diese personenbezogenen Daten werden vom Auftragnehmer als Verantwortlichem verarbeitet, um den Benutzern die Nutzung der Software zu ermöglichen. Hinsichtlich der diesbezüglichen Betroffenenrechte und sonstiger Informationspflichten wird auf die Datenschutzerklärung auf der Internetseite des Auftragnehmers verwiesen.

**10.2** Der Auftragnehmer ist berechtigt, anonymisierte Daten im Zusammenhang mit der Nutzung der Software für interne Geschäfts- und/oder Betriebszwecke zu verwenden, insbesondere zur Analyse der Nutzung der Software und zur Verbesserung der Software. Der Auftraggeber erteilt eine entsprechende Weisung zur Anonymisierung der hierfür erforderlichen Daten.

**10.3** Der Auftragnehmer ist berechtigt, auf die Software zuzugreifen, um die Einhaltung der Nutzungsbedingungen der Software, inklusive der Vergütung, durch den Auftraggeber zu verifizieren; um Diagnosen und Analysen zu erstellen und um die Einstellungen der Software anzupassen und zu optimieren, um die Leistung und/oder Sicherheit der Software zu verbessern, vorausgesetzt dass diese Anpassungen keine

negativen Auswirkungen auf die Nutzung der Software durch den Auftraggeber haben. Der Auftragnehmer ist des Weiteren berechtigt, System-/Metadaten über die Nutzung der Software zu erheben, um diese im Rahmen der Identifikation und Behebung potentieller Mängel und Fehler der Software zu nutzen, um statistische Analysen zu erstellen und um die Entwicklung der Software zu unterstützen und zu optimieren.

**10.4** Im Rahmen der Nutzung der Software kann der Auftraggeber personenbezogene Daten verarbeiten. Der Auftraggeber ist dabei Verantwortlicher und der Auftragnehmer ist ein Auftragsverarbeiter. Diese Auftragsverarbeitung ist in der Vereinbarung Auftragsverarbeitung zwischen den Parteien geregelt, die als Anlage 1 ausdrücklich in den Vertrag zwischen den Parteien einbezogen wird.

## **11 Laufzeit**

**11.1** Die initiale Laufzeit wird in der Bestellung vereinbart. Die Laufzeit verlängert sich jeweils um die Dauer der initialen Laufzeit, sofern die jeweilige Bestellung nicht mit einer Frist von drei Kalendermonaten zum Ende der jeweiligen Laufzeit schriftlich gekündigt wird.

**11.2** Verträge sind von jeder Partei jederzeit kündbar im Falle einer wesentlichen Vertragsverletzung der jeweils anderen Partei, wenn die Vertragsverletzung nicht innerhalb von 30 Tagen geheilt wird. Diese Frist beginnt ab dem Zeitpunkt der Zustellung der schriftlichen Anzeige der wesentlichen Vertragsverletzung.

**11.3** Jede Partei kann den Vertrag jederzeit fristlos kündigen, wenn die andere Partei in Liquidation geht oder ein Insolvenzantrag gestellt und nicht innerhalb von vier Wochen ab Antragstellung zurückgenommen wurde.

## **12 Sonstiges**



**12.1** Dieser Vertrag unterliegt deutschem Recht. Im Falle von Meinungsverschiedenheiten aufgrund dieses Vertrages verpflichten sich die Parteien, zunächst eine gütliche Einigung zu finden. Sollte dies nicht möglich sein, so einigen sich die Parteien bereits jetzt auf Göppingen als allgemeinen Gerichtsstand.

**12.2** Für Nebenabreden ist die Schriftform erforderlich. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht. Alle Mitteilungen unter diesem Vertrag bedürfen der Schriftform und werden mit erster Zustellung wirksam.

**12.3** Der Auftragnehmer kann Änderungen an diesen AGB vornehmen, wenn diese aufgrund geänderter Umstände, beispielsweise bei wesentlichen Änderungen der Gesetzgebung oder der Rechtsprechung, des relevanten Markt- und Geschäftsumfelds oder aufgrund technischer Entwicklungen notwendig werden und für den Auftraggeber zumutbar sind. Der Auftragnehmer wird den Auftraggeber in einem angemessenen Zeitraum, mindestens einen Monat, vor Inkrafttreten der Änderungen, über die Änderungen in elektronischer Form informieren. Der Auftraggeber ist berechtigt, solchen Änderungen innerhalb von 14 Tagen nach Erhalt der Änderungsmitteilung zu widersprechen. Im Falle eines Widerspruchs des Auftraggebers hat der Auftragnehmer das Recht, das Vertragsverhältnis außerordentlich ohne Einhaltung einer Kündigungsfrist zu kündigen. Widerspricht der Auftraggeber nicht, gilt seine Zustimmung nach Ablauf der oben genannten Fristen als erteilt. Auf die Dauer der Frist und auf die Bedeutung ihres ergebnislosen Ablaufs wird der Auftragnehmer bei der Ankündigung der Änderungen dieser AGB ausdrücklich hinweisen.

## Vereinbarung Auftragsverarbeitung

### 1. Allgemeines

Der Auftragnehmer stellt dem Auftraggeber seine Plattform als Software as a Service (SaaS) zur Verfügung. Mit der Software kann der Auftraggeber personenbezogene Daten erheben und verarbeiten. Dementsprechend beinhaltet der von den Parteien geschlossene Vertrag über die Zurverfügungstellung der Software („Hauptvertrag“) die Verarbeitung von personenbezogenen Daten im Auftrag durch den Auftragnehmer. Diese Vereinbarung Auftragsverarbeitung („AVV“) konkretisiert, als Teil des Hauptvertrages, die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts, insbesondere der Anforderungen der Datenschutz-Grundverordnung („DSGVO“).

### 2. Anwendungsbereich

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind im Hauptvertrag und in **Anlage 1 zu dieser AVV** festgelegt. Die Laufzeit dieser AVV und die Dauer der Auftragsverarbeitung entsprechen der Laufzeit des Hauptvertrages.

### 3. Weisungsgebundenheit

**3.1** Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Dies betrifft auch die Übermittlung in Drittländer ohne angemessenes Datenschutzniveau. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

**3.2** Falls der Auftragnehmer verpflichtet ist, personenbezogene Daten nach dem Recht der Europäischen Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, zu verarbeiten, wird der Auftragnehmer den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Verantwortlichen unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

**3.3** Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

**3.4** Der Auftragnehmer darf Daten über die Nutzung der Software durch den Auftraggeber in anonymisierter Form zum Zwecke der Optimierung der Software, der User Experience und für sicherheitsrelevante Auswertungen verwenden. Der Auftraggeber erteilt hiermit eine entsprechende Weisung für die entsprechende Anonymisierung.

### 4. Technische und organisatorische Maßnahmen

**4.1** Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

**4.2** Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist in **Anlage 2 zu dieser AVV** dokumentiert. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftraggeber kann jederzeit eine aktuelle Übersicht der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

## **5. Betroffenenrechte**

**5.1** Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO (insb. Auskunft, Berichtigung, Sperrung oder Löschung). Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

**5.2** Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

## **6. Sonstige Pflichten des Auftragnehmers**

**6.1** Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

**6.2** Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie erforderlichenfalls bei Durchführung einer Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung unverzüglich zur Verfügung zu stellen.

**6.3** Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

**6.4** Die beim Auftragnehmer zur Verarbeitung eingesetzten Personen haben sich schriftlich zur Vertraulichkeit verpflichtet, wurden mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht und werden hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht.

**6.5** Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützen.

## **7. Rechte und Pflichten des Auftraggebers**

**7.1** Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

**7.2** Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer, soweit erforderlich und möglich, Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

## **8. Unterauftragsverarbeiter**

**8.1** Die Beauftragung von Unterauftragsverarbeitern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers zulässig. Der Auftraggeber stimmt der Beauftragung von Unterauftragsverarbeitern gemäß der Übersicht Unterauftragsverarbeiter, anbei als **Anlage 3 zu dieser AVV**, zu. In der Übersicht Unterauftragsverarbeiter ist auch der Prozess für zukünftige Änderungen der Unterauftragsverarbeiter definiert.

**8.2** Der Auftragnehmer hat die Unterauftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten können. Der Auftragnehmer hat insbesondere zu kontrollieren, dass sämtliche Unterauftragsverarbeiter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben.

**8.3** Nicht als Unterauftragsverarbeitung im Sinne dieser AVV sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben.

**8.4** Die Beauftragung von Unterauftragsverarbeitern lässt die vertraglichen und datenschutzrechtlichen Verpflichtungen des Auftragnehmers gegenüber dem Auftraggeber unberührt. Der Auftragnehmer haftet für eventuelle Schlechtleistungen eines Unterauftragsverarbeiters wie für eigenes Verschulden.

## **9. Löschung und Rückgabe von personenbezogenen Daten**

**9.1** 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 erforderlich sind.

**9.2** Nach Beendigung der Leistungsvereinbarung oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer die im Auftrag verarbeiteten personenbezogenen Daten dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen.

**9.3** Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

## **10. Schlussbestimmungen**

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

## **Anlage 1 zur Vereinbarung Auftragsverarbeitung: Beschreibung der Auftragsverarbeitung**

### **1. Gegenstand, Art und Zweck der Verarbeitung**

Der Auftragnehmer stellt dem Auftraggeber die mhi-Plattform mhi regio website als SaaS zur Verfügung. Er wird dabei als Auftragsverarbeiter für den Auftraggeber tätig. Der im Hauptvertrag bezeichnete Auftraggeber ist Verantwortlicher im Sinne der DSGVO und nutzt die mhi regio des Auftragnehmers zur Erhebung und Verarbeitung personenbezogene Daten.

### **2. Betroffene Personen**

Die im Auftrag verarbeiteten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Kunden und Interessenten des Händlers
- Website-Besucher

### **3. Kategorien von Daten**

Die im Auftrag verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- IP-Adresse
- Geschlecht
- Name
- Adresse
- E-Mail-Adresse

### **4. Dauer der Auftragsverarbeitung**

Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages.



## **Anlage 2 zur Vereinbarung Auftragsverarbeitung:**

### **Technische und organisatorische Maßnahmen**

#### **1. Vertraulichkeit**

##### **1.1 Zutrittskontrolle**

###### **Hosting/Rechenzentrum:**

Das Hosting der Software erfolgt in Rechenzentren in München. Das Rechenzentrum ist nach ISO27001 zertifiziert.

###### **Büroräume:**

Die Büroräume des Auftragnehmers befinden sich in einem Bürohaus. Die Zugänge zum Bürohaus und auch zu den Büroräumen des Auftragnehmers sind Tag und Nacht verschlossen. Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Es kommt ein Schließsystem zum Einsatz, das vom Vermieter verwaltet wird. Jeder Mieter des Bürohauses hat jedoch die Möglichkeit, die jeweils ausgehändigten Schlüssel selbst zu verwalten und Zutrittsrecht zu erteilen und zu entziehen. Dies wird von der Personalabteilung des Auftragnehmers verwaltet.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu dem Bürohaus und dann den Büroräumen.

Jeder Besucher wird in einem Besucherbuch protokolliert und dann von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet.

Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

##### **1.2 Zugangskontrolle**

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde.

Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet sind ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

### **1.3 Zugriffskontrolle**

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden ausschließlich von Administratoren eingerichtet.

Berechtigungen werden immer strikt nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine ordnungsgemäße Vernichtung gewährleistet.

Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

### **1.4 Trennung**

Alle vom Auftragnehmer für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die logische Zuordnung der im Auftrag eines Kunden verarbeiteten Daten zu dem jeweiligen Kunden und damit die logische Trennung der Daten ist stets gewährleistet.

### **1.5 Pseudonymisierung & Verschlüsselung**

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

## **2. Integrität**

### **2.1 Eingabekontrolle**

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die vom Auftragnehmer im Auftrag verarbeitet werden, wird protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

### **2.2 Weitergabekontrolle**

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden des Auftragnehmers erfolgt, darf jeweils nur in dem Umfang, wie erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten des Auftragnehmers im Zusammenhang mit Kundenprojekten untersagt.

Mitarbeiter des Auftragnehmers werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

## **3. Verfügbarkeit und Belastbarkeit**

Die Daten auf den Systemen des Auftragnehmers werden regelmäßig in Form von Backups gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht. Das Einspielen von Backups wird regelmäßig getestet.

Die Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Rechenzentrum befinden sich eine Brandmeldeanlage sowie eine Löschanlage. Alle Systeme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es besteht ein Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

#### **4. Auftragskontrolle**

Die Software des Auftragnehmers wird in der Europäischen Union gehostet.

Beim Auftragnehmer ist ein betrieblicher Datenschutzbeauftragter benannt.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführtem Audit durch den Datenschutzbeauftragten des Auftragnehmers abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

#### **5. Privacy by Design und Privacy by Default**

Es wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit Rechnung getragen wird. Die Art der Datenerhebung mittels der Software und die zu erhebenden Datenkategorien können vom Auftraggeber individuell angepasst und verwaltet werden.

Die Software des Auftragnehmers unterstützt die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

#### **6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

Der Auftragnehmer hat ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt. Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

### Anlage 3 zur Vereinbarung Auftragsverarbeitung: Übersicht Unterauftragsverarbeiter

Der Auftragnehmer setzt bei der Erbringung der Leistungen aus dem Hauptvertrag folgende Unterauftragsverarbeiter ein:

Unterauftragsverarbeiter	Leistungen des Unterauftragsverarbeiter	Ort der Datenverarbeitung
<b>ATRIVIO GmbH</b>	Hosting der Software E-Mail-Service-Provider Versand von Transaktionsnachrichten	Deutschland
<b>e-vendo AG</b>	Hosting der Portalsoftware Hosting der Produktseiten der Händlerwebsite Bereitstellung des Händlerportals	Deutschland
<b>KlickPiloten GmbH</b>	Online-Marketing Digital-Analytics Beratung	EU

Der Auftragnehmer kann die Beauftragung einzelner Unterauftragsverarbeiter beenden oder zusätzliche Unterauftragsverarbeiter beauftragen.

Der Auftragnehmer wird den Auftraggeber bei der Beauftragung zusätzlicher Unterauftragsverarbeiter auf elektronischem Wege mindestens 30 Tage vor Einsatz des zusätzlichen Unterauftragsverarbeiters über dessen geplanten Einsatz informieren. Ausgenommen hiervon sind Notfallersetzungen wie weiter unten definiert.

Sollte der Auftraggeber einen wesentlichen Grund haben, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen, wird der Auftraggeber dies dem Auftragnehmer spätestens 15 Tage nach der Information über den geplanten Einsatz des Unterauftragsverarbeiters schriftlich und unter Nennung des wesentlichen Grundes mitteilen. Sollte der Auftraggeber innerhalb dieser Zeitspanne nicht widersprechen, so wird der Einsatz des zusätzlichen Unterauftragsverarbeiters als vom Auftraggeber genehmigt angesehen.

Sollte der Auftraggeber widersprechen, kann der Auftragnehmer den Widerspruch wie folgt heilen: (1.) Der Auftragnehmer wird den zusätzlichen Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten des Auftraggebers nicht einsetzen, oder (2.) der Auftragnehmer wird Maßnahmen ergreifen, um den wesentlichen Grund für den Widerspruch des Auftraggebers auszuräumen, oder (3.) der Auftragnehmer kann die Erbringung des von dem Einsatz des zusätzlichen Unterauftragsverarbeiters betroffenen Aspekts der Leistung gegenüber dem Auftraggeber vorübergehend oder dauerhaft einstellen und dem Auftraggeber die für die Erbringung des Aspekts der Leistung eventuell bereits vorab gezahlte Vergütung zurückerstatten. Sollte keine dieser drei Optionen machbar sein und wurde dem Widerspruch nicht innerhalb von 15 Tagen nach Zugang des Widerspruchs abgeholfen, kann jede Partei den Vertrag mit angemessener Frist außerordentlich kündigen.

Notfallersetzungen eines Unterauftragsverarbeiters können erforderlich werden, wenn die Erforderlichkeit des sofortigen Einsatzes eines zusätzlichen Unterauftragsverarbeiters außerhalb der Kontrolle des Auftragnehmers liegt, beispielsweise wenn ein Unterauftragsverarbeiter überraschend den Geschäftsbetrieb einstellt oder seine wesentlichen Vertragspflichten gegenüber dem Auftragnehmer verletzt, so dass es dem Auftragnehmer nicht mehr möglich ist/wäre, die gegenüber dem Auftraggeber geschuldete Leistung zu erbringen. In einem solchen Fall wird der Auftragnehmer den Kunden unverzüglich über den zusätzlichen Unterauftragsverarbeiter informieren und der Widerspruchsprozess, wie oben definiert, wird mit der Information des Auftraggebers eingeleitet.