Vertrag über die Verarbeitung von Daten im Auftrag

zwischen

X GmbH
X-Straße 123
12345 Musterstadt

- Auftraggeber -

und

Mauve Mailorder Software GmbH & Co. KG, Laurentiusweg 83, 45276 Essen

- Auftragnehmer –

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(5) 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. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des

Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- 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;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

(4) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

8. Kontrollbefugnisse

(1) Der Auftraggeber überzeugt sich vor Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragverarbeiters. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers prüfen oder durch beauftragte Dritte prüfen lassen.

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

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach rechtzeitiger Abstimmung durchgeführt.

(5) Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte

Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(5) Der Auftragsverarbeiter erhält vom Auftraggeber für eigene Mitwirkungsleistungen im Rahmen einer Prüfung eine Aufwandsentschädigung nach Maßgabe der jeweils gültigen Preisliste des Auftragsverarbeiters. Insbesondere die notwendige Anwesenheit der Mitarbeiter des Auftragnehmers sowie des Datenschutzbeauftragten sind zu ersetzen.

(6) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

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

(2) Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben.

(3) Der Auftragnehmer hat den Subunternehmer 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 Subunternehmer die nach Art. 32 DSGVO 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 Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DSGVO bestellt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Subunternehmer bestellt ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Der Auftragnehmer hat dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer kann weitere Unterauftragnehmer hinzuziehen, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit (mindestens 2 Wochen) vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. 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. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - 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.

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

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages 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 soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) 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. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(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.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag 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 Voraus 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.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und gilt für die Dauer des jeweiligen Hauptvertrages.

(2) Ein außerordentliches Kündigungsrecht jeder Partei bleibt hiervon unberührt.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder nach vorheriger Zustimmung datenschutzgerecht zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) 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.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum 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.

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

_____, den	_____	_____, den	_____
Ort	Datum	Ort	Datum
_____		_____	
- Auftraggeber -		- Auftragnehmer -	

Anlage 1 - Gegenstand des Auftrags

Art. 32 DSGVO: Sicherheit der Verarbeitung

Art. 32 DS-GVO bestimmt, dass die verantwortliche Stelle technische- und organisatorische Maßnahmen treffen muss. Diese müssen unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen werden. Diese Maßnahmen müssen die Pseudonymisierung, die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit als auch die Fähigkeit, Systeme nach einem Zwischenfall rasch wiederherstellen zu können, mit einbeziehen.
Weiter muss ein Verfahren implementiert werden, was die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen gewährleistet.
Die folgenden technischen- und Organisatorischen Maßnahmen wurden durch die Mauve Mailorder Software GmbH & Co. KG getroffen. Im Rahmen der technischen und organisatorischen Maßnahmen werden die von Mauve Mailorder Software GmbH & Co.KG getroffenen Maßnahmen, als auch die des Rechenzentrums der Hetzner Online GmbH im Rahmen des bereitgestellten Data-Housings beschrieben.

I. Vertraulichkeit

Vertraulichkeit bedeutet, dass die Daten nur von befugten Personen erhoben, verarbeitet, genutzt usw. werden dürfen.
Die Vertraulichkeit der Datenverarbeitung wird durch die folgenden Maßnahmen gesichert:

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☒ Alarmanlage	☒ Chip-/Transponder-Schließsystem
☒ Videoüberwachung Zugänge	☒ Sicherheitsschlösser
☒ Besetzter Empfang / Pförtner	☒ Protokollierung Besucher
☒ Ausweisregelung für Besucher	
☒ Schlüsselkonzept Serverraum	☒ verschlossener Serverschrank

☒ Notstromaggregat	☒ USV
☒ Klimaanlage	
☒ sorgfältige Auswahl Reinigungspersonal	☒ sorgfältige Auswahl Wachpersonal
Weitere: Die Daten werden in einem Rechenzentrum der Hetzner Online GmbH im Rahmen eines Server-Housings bereitgestellt. Im Rechenzentrum existieren Sicherheitsmaßnahmen, um den Zutritt zum Gelände und den Serveranlagen zu reglementieren. So ist das Gelände mit einem Hochsicherheitszaun geschützt, die Zugänge zum Gelände sind videoüberwacht, an den Ein- und Ausgängen gibt es Sicherheitsschleusen. Betriebsfremde Personen dürfen sich nur in Begleitung eines Mitarbeiters der Hetzner Online GmbH auf dem Gelände aufhalten.	

2. Zugangskontrolle

Durch die Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Auf die Serverumgebung selbst können nur die IT zugreifen.

☒ Zuordnung von Benutzerrechten	☒ Erstellen von Benutzerprofilen
☒ Passwortvergabe	☒ Anmeldung mit Benutzername/Passwort
☒ Einsatz einer Softwarefirewall	☒ Sperren bestimmter Ports
☒ Einsatz von VPN-Verbindungen	☒ Verschlüsselung von Datenträgern
☒ Verschlüsselung von Datenträgern	
weitere: Die Daten werden im Rechenzentrum lediglich im Rahmen eines Server-Housings bereitgestellt. Der Betreiber des Rechenzentrums selbst hat keinerlei Möglichkeiten, auf die bei ihm liegenden Daten zuzugreifen. Der Betreiber stellt lediglich die technische Infrastruktur zur Verfügung und gewährleistet die technische Sicherheit.	

3. Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, 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, verändert oder entfernt werden können.

☒ Rollenberechtigungskonzept	☒ Rechteverwaltung durch Admin

☒ Anzahl Adminrollen so gering wie möglich	☒ Passwortrichtlinie
☒ Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung, Löschung von Daten)	☒ Sichere Aufbewahrung von Datenträgern
☒ Verschlüsselung von Datenträgern	☒ Automatisches Ausloggen bei Inaktivität (z.B. Bildschirmsperre bei Abwesenheit)
☒ ordnungsgemäße Vernichtung von Datenträgern	
weitere: Ein Zugriff seitens des Rechenzentrums findet nicht statt, da die Server im Rahmen eines Serverhousings bereitgestellt werden.	

4. Trennungsgebot

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

☒ logische Mandantentrennung	
☒ Festlegung von Datenbankrechten	☒ Trennung Produktiv- und Testsystem
weitere: Im internen Verwaltungssystem des Rechenzentrums werden die Datenbestände logisch und physisch voneinander getrennt aufbewahrt. Im Rahmen der Bereitstellung des Rechenzentrums obliegt die Trennungskontrolle beim Auftraggeber.	

5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugeordnet werden. (Art. 4 Nr. 5 DS-GVO).

Prozesse, die mit personenbezogenen Daten arbeiten, sind bereits von Anfang an datenschutzfreundlich zu gestalten; die Pseudonymisierung kann hierfür ein wichtiger Bestandteil sein.

☒ Pseudonymisierte Nutzung von Tracking-Tools
weitere: Aufgrund der spezifischen Tätigkeit ist die Pseudonymisierung nicht geeignet, das Risiko für die Rechte und Freiheiten des von der Verarbeitung Betroffenen zu senken. Das Risiko wird durch die anderen ergriffenen technischen und organisatorischen Maßnahmen minimiert. Soweit Analyse- und Trackingverfahren im Netz eingesetzt werden, erfolgt die Auswertung pseudonymisiert.

II. Integrität

Integrität bedeutet, dass die Systeme und die dort hinterlegten Daten korrekt, unverändert, und verlässlich sind.

Die Integrität der Daten wird durch folgende Maßnahmen sichergestellt:

1. Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

☒ Protokollierung von Stammdatenänderungen	☒ Logfilekontrolle
☒ Vergabe von Änderungs- Lösch- und Bearbeitungsrechten aufgrund eines Rollenberechtigungskonzeptes	☒ Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch individuelle Nutzer
☒ Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung, Löschung von Daten)	☒ Protokollierung der Serveraktivitäten
☒ Protokollierung gescheiterter Zugriffsversuche	
weitere: Im Rahmen des Serverhousings obliegt die Eingabekontrolle beim Auftraggeber.	

2. Weitergabekontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung

auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☒ VPN-Tunnel bei externen Geräten
weitere: Der Übertragungsweg der E-Mails ist per TLS verschlüsselt. Das Rechenzentrum stellt verschlüsselte Übertragungsmöglichkeiten bereit. Weiter sind die Mitarbeiter im Rechenzentrum nach Art 32 IV DS-GVO unterwiesen und auf den datenschutzkonformen Umgang hingewiesen worden.

3. Auftragskontrolle

Durch die Auftragskontrolle wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten	☒ vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
☒ schriftliche Weisungen an den Auftragnehmer	☒ Verpflichtung Mitarbeiter des Auftragnehmers auf den Datenschutz / Verschwiegenheitspflichten
☒ Auftragnehmer hat Datenschutzbeauftragten bestellt (wenn gesetzlich vorgeschrieben)	☒ Sicherstellung der Vernichtung von Daten nach Vertragsende
☒ Kontrollrechte gegenüber dem Auftragnehmer	☒ laufende Kontrolle des Auftragnehmers
weitere: Die Anfragen im Haus werden durch ein Ticketsystem bearbeitet, so dass der Bearbeitungsstand nachgehalten werden kann. Im Übrigen wird versucht, die Zahl der Unterauftragnehmer so gering wie möglich zu halten. Sollte die Hinzuziehung von weiteren Dienstleistern nicht ausgeschlossen werden können, müssen diese sich im Rahmen von Auftragsverarbeitungsverträgen Weisungs- und Kontrollrechten unterwerfen. Das Rechenzentrum hat einen Datenschutzbeauftragten und einen Informationssicherheitsbeauftragten bestellt. Die Tätigkeiten und das Weisungsrecht gegenüber dem Rechenzentrum sind in entsprechenden Verträgen vereinbart worden.	

III. Verfügbarkeit und Belastbarkeit

Verfügbarkeit bedeutet, dass Daten zur Verfügung stehen, wenn sie gebraucht werden.

Das Schutzziel „Belastbarkeit“ wird nicht in der DS-GVO legaldefiniert und hat auch keine Entsprechung im IT-Grundschutz. Nach gegenwärtiger Auffassung ist unter „Belastbarkeit“ die Widerstandsfähigkeit von Systemen gemeint, wie sie im Bereich des Notfallmanagements eine Rolle spielt.

Diese Schutzziele werden durch die folgenden Maßnahmen sichergestellt:

1. Verfügbarkeitskontrolle

Durch die Verfügbarkeitskontrolle wird gewährleistet, dass personenbezogene Daten gegen den zufälligen Verlust geschützt sind.

☒ USV	☒ Klimaanlage in Serverräumen
☒ Temperaturüberwachung / Feuchtigkeitsüberwachung in Serverräumen	☒ Videoüberwachung im Serverraum
☒ Schutzsteckdosenleisten in Serverräumen	☒ Feuer- und Rauchmeldeanlagen
☒ Alarmmeldung bei unberechtigten Zutritten zu den Serverräumen	☒ Backup- und Recoverykonzept
☒ Testen von Datenwiederherstellung	☒ Serverräume nicht unter sanitären Anlagen
☒ Aufbewahrung von Datensicherungen im anderem Brandabschnitt	☒ Spiegelung der Systeme
☒ Regelmäßige Erstellung von Sicherheitskopien	
weitere: Da das Rechenzentrum keinen Zugriff auf die Daten hat, obliegt die Verfügbarkeitskontrolle beim Auftraggeber. Dass Rechenzentrum stellt soweit aber eine unterbrechungsfreie Stromversorgung als auch eine Netzersatzanlage zur Verfügung. Weiterhin sind die Systeme gegen DDoS-Attacken geschützt.	

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die getroffenen Maßnahmen müssen einer regelmäßigen Kontrolle unterzogen werden. Auch sind sie dem jeweils entsprechenden Stand der Technik anzupassen und aktuell zu halten. Im Unternehmen wird ein solches regelmäßiges Kontroll- und Evaluierungskonzept wie folgt umgesetzt:

- ☒ Regelmäßige Mitarbeiterschulungen- und Prüfungen
- ☒ Regelmäßige Prüfung der technischen Komponenten und des Backup- und Recoverykonzepts
- ☒ interne Verhaltensregeln
- ☒ Allgemeine Datensicherheitsbeschreibung
- ☒ Wiederanlaufkonzept

weitere: Die Prozesse im Haus werden regelmäßig auf ihre datenschutzrechtliche Kongruenz hin regelmäßig auditiert. Die Mitarbeiter sind auf die Einhaltung des Datenschutzes verpflichtet worden. Bestimmte notwendige Sicherheitskonzepte werden im Haus nachgehalten. Das Rechenzentrum der Hetzner Online GmbH ist nach ISO 27001 zertifiziert.

Anlage 2 - Unterauftragnehmer

Art. 32 DSGVO: Sicherheit der Verarbeitung

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Caesar & Gustav UG	Rotenbergstr. 39 70190 Stuttgart	Webdesign und Funktionalität
Marco Puppe & Kian Foroodi GbR	Colmarer Str. 12 65203 Wiesbaden	Webdesign und Funktionalität