

DIGITAL MARKETING ADDENDUM

1. VERTRAGSGEGENSTAND

Dieses Digital Marketing Addendum findet Anwendung auf die Zurverfügungstellung und Nutzung von MAPP Software, wie etwa des Digital Marketing Center (DMC), für digitale Marketingdienstleistungen, insbesondere, aber nicht nur digitales Direktmarketing durch elektronische Post und für jede Art von Versand.

2. DEFINITIONEN

- 2.1 „Adresse“ umfasst in der Bedeutung dieses Vertrages E-Mail-Adressen, Mobilfunknummern, Faxnummern oder jede andere Art von elektronischer Adressen.
- 2.2 „Adressliste“ oder „Liste“ meint eine Liste von Adressen, welche zum Versand via DMC geeignet ist.
- 2.3 „Deliverability“ meint die Fähigkeit, E-Mail-Nachrichten in den Posteingang des Empfängers zu liefern und es dabei zu vermeiden, dass E-Mails nicht ausgeliefert, blockiert oder für SPAM gehalten werden. Deliverability wird im Folgenden auch als Zustellbarkeit bezeichnet.
- 2.4 „ISP“ bedeutet E-Mail- und Web-Mail-Service-Provider, wie etwa HoMappil, GMX oder Gmail.
- 2.5 „Nachricht“ meint eine elektronische Nachricht. Dies umfasst, ist aber nicht begrenzt auf E-Mails, Fax, SMS/MMS, Push-Nachrichten, In-App-Nachrichten, Instant Messages und Nachrichten, Posts oder Hinweise auf Social-Media-Plattformen.
- 2.6 „Rejected Bounce“ ist die Mitteilung des angeschriebenen Mailservers, dass die angeschriebene Adresse nicht existiert oder dauerhaft deaktiviert ist.
- 2.7 „Spam Complaint“ ist die Mitteilung eines ISPs, dass eine über DMC versendete E-Mail von einem Adressaten als „Junk“ oder „Spam“ markiert wurde.
- 2.8 „Versand“ meint das Aussenden von Nachrichten an bestimmte Adressen oder Listen durch das DMC-System.
- 2.9 „Werktag“ meint einen Tag, der weder Samstag, noch Sonntag ist, noch ein Feiertag am Ort der Niederlassung von MAPP.

3. BEREITSTELLUNG UND NUTZUNG DES DMC

- 3.1 MAPP stellt dem Auftraggeber ein DMC-System unter einer Subdomain seiner Wahl (z.B. newsletter.kunde.com) zur Verfügung. Die Subdomain hat der Auftraggeber mindestens 5 Werktage vor dem geplanten System-Setup an die Server von MAPP zu delegieren.
- 3.2 Die unverschlüsselte Übertragung von Daten kann eine Gefährdung der Vertraulichkeit dieser Daten bedeuten. Daher sind Daten, die an MAPP für den Import in DMC übermittelt werden, vom Auftraggeber über eine sichere Verbindung (z. B. sFTP) zur Verfügung zu stellen. Daten, welche vom Auftraggeber zur Verfügung gestellt werden, sollen nur innerhalb der sicheren DMC-Umgebung gespeichert werden. Aus Sicherheitsgründen werden die Daten auf FTP/sFTP-Servern regelmäßig gelöscht.
- 3.3 Die Speicherung von Informationen und Auswertungen eines Versands erfordert große Speicherkapazität. Solche Informationen und Auswertungen werden für zwölf Monate nach dem Versandzeitpunkt archiviert. Ein direkter Zugriff auf archivierte Daten über DMC ist nicht möglich. Der Zugriff auf archivierte Daten und Backups kann vom Auftraggeber kostenpflichtig gemäß der aktuellen Stundensätze beauftragt werden. Bilder, Graphiken und andere Anhänge zu Nachrichten werden sechs Monate nach dem Versand gelöscht.
- 3.4 Alle vom Auftraggeber zur Verfügung gestellten Daten werden auf Weisung des Auftraggebers und bei Beendigung des Vertrages unverzüglich aus dem DMC-System des Auftraggebers gelöscht. Die Löschung aus dem DMC System hat keinen Einfluss auf Sicherheitskopien im Backup des DMC Systems. Im Falle der Beendigung des Vertrages sollte der Auftraggeber seine in DMC gespeicherten Datenbestände bis zum Zeitpunkt der Beendigung des Vertrages durch Download und Export bei sich sichern, da mit Beendigung des Vertrages ein Zugriff auf das System nicht mehr gewährleistet wird. Allein der Auftraggeber ist verantwortlich für die ihm obliegenden Aufbewahrungsfristen, MAPP ist nicht verpflichtet, Daten oder Dokumente für den Auftraggeber vorzuhalten oder aufzubewahren.
- 3.5 MAPP hat das Recht, Versandvorgänge aggregiert und anonymisiert auszuwerten, diese Auswertungen für statistische Zwecke und für Zwecke der Marktforschung zu verwenden (wie etwa die Auswertung der Öffnungsrate von Newslettern im FMCG Sektor) und zu veröffentlichen. Es werden bei diesen Auswertungen keine personenbezogenen Daten verarbeitet. Bei Veröffentlichungen wird der Auftraggeber unkenntlich gemacht.

4. COMPLIANCE POLICY

- 4.1 Der Auftraggeber hat sich bei der Nutzung von DMC, inklusive verbundener Dienstleistungen, wie das Website Hosting, dem Versand von Nachrichten und der Datenverarbeitung durch DMC an die jeweils anwendbaren rechtlichen Vorschriften zu halten. Der Auftraggeber ist hierbei allein verantwortlich, sich über das jeweils geltende Recht, dessen

Auslegung und Anwendung sowie die anwendbaren Industriestandards zu informieren und diese einzuhalten. Hierzu kann es notwendig sein, dass der Auftraggeber die Voreinstellungen der Software verändern muss.

- 4.2 MAPP ist nicht verpflichtet, dem Auftraggeber DMC zur Verfügung zu stellen oder einen Versand durchzuführen, sollte sich der Auftraggeber bei dem Versand von Nachrichten nicht rechtskonform verhalten oder gängige Industriestandards und Best-Practice-Empfehlungen missachten.
- 4.3 Werbliche Nachrichten dürfen nur dann über DMC versendet werden, wenn der Adressat ausdrücklich in den jeweiligen Versand eingewilligt hat und/oder die Zusendung von werblichen E-Mails ansonsten rechtskonform und in Übereinstimmung mit den geltenden Industriestandards und Best-Practice-Empfehlungen erfolgt. Einwilligungserklärungen müssen inhaltlich und formell den rechtlichen Anforderungen genügen, dokumentiert werden und nachweisbar sein. Der werbliche Charakter der werblichen E-Mails darf nicht verschleiert oder verborgen werden. Für die Erhebung von Einwilligungen wird ausdrücklich die Verwendung des Double-Opt-In-Verfahrens empfohlen.
- 4.4 Werbliche Nachrichten müssen Kontaktinformationen des Auftraggebers gemäß anwendbaren Rechts enthalten und einen Abmelde-Link oder eine sonstige Kontaktmöglichkeit enthalten, mittels derer der Adressat seine Einwilligung widerrufen kann. Widerrufe, die über die Unsubscribe-Funktion von DMC erfolgen, werden von DMC automatisiert umgesetzt. Andere Widerrufsmöglichkeiten dürfen den Widerruf nicht übermäßig erschweren, d. h. es darf insbesondere kein Login erforderlich sein. Widerrufe, die direkt an den Auftraggeber gerichtet werden, müssen von diesem innerhalb von drei Werktagen umgesetzt werden. Der Auftraggeber muss sicherstellen, dass alle E-Mails an die angegebene From- und Reply-Adresse unverzüglich bearbeitet werden. Einige E-Mail- bzw. Freemail-Provider („ISPs“) informieren MAPP, wenn eine über DMC versendete E-Mail vom Adressaten als „Junk“ oder „Spam“ markiert wird (so genannter Feedback-Loop). Diese Markierung wird von DMC als Widerruf gewertet und dieser Widerruf entsprechend umgesetzt.
- 4.5 Resultiert aus der Versendung einer Nachricht des Auftraggebers eine Beschwerde eines Adressaten an MAPP, ein Blacklisting bei einer Anti-Spam-Organisation (z.B. Spamhaus oder Spamcop) oder erhält MAPP eine Anfrage einer Aufsichtsbehörde oder eines relevanten Verbandes (z.B. CSA), muss der Auftraggeber MAPP innerhalb eines Werktages den Nachweis der Rechtmäßigkeit des Versandes erbringen. MAPP ist hierbei berechtigt, diesen Nachweis Dritten gegenüber offenzulegen, soweit dies erforderlich ist.
- 4.6 Der Auftraggeber ist verpflichtet, (i) keine Inhalte zu versenden, zu übermitteln, zu speichern, zu verlinken oder auf sonstige Art und Weise auf Inhalte hinzuweisen, die pornographischer oder gegen Jugendschutzgesetze verstoßender, implizit oder explizit sexuell anzüglicher, gewaltverherrlichender, persönlichkeitsrechts-verletzender, bedrohender, beleidigender, belästigender, verleumderischer, betrügerischer, vulgärer, obszöner, hasserregender, links- oder rechtsextremistischer Natur sind oder die zum Verstoß gegen Gesetze auffordern oder anstiften, (ii) keine Inhalte zu übermitteln, zu speichern, zu verlinken oder auf sonstige Art und Weise auf Inhalte weisen, die Rechte Dritter, insbesondere Marken-, Kennzeichen- und Urheberrechte, Patente, Geschmacks- und Gebrauchsmuster und Geschäftsgeheimnisse, verletzen und (iii) keine schädlichen Programme (wie z. B. Viren) zu übermitteln, zu speichern, zu verlinken oder auf sonstige Art und Weise auf schädliche Programme hinzuweisen.
- 4.7 DMC bietet umfangreiche Funktionalitäten (z.B. Kampagnentracking, Bildung von Nutzerprofilen und Targeting), auf deren Einsatz der betroffene Adressat unter Umständen hinzuweisen ist oder für deren Einsatz die ausdrückliche Einwilligung des betroffenen Adressaten erforderlich sein kann. Der Auftraggeber hat zu gewährleisten, dass die Nutzung der verschiedenen Funktionalitäten des Services hinsichtlich der betroffenen Daten bzw. E-Mail-Adressen rechtskonform erfolgt. Der Auftraggeber hat die Default-Einstellungen von DMC diesbezüglich mit seinen Anforderungen abzugleichen. Es ist Aufgabe des Auftraggebers, eventuell notwendige Genehmigungen von zuständigen Behörden einzuholen.
- 4.8 Der Auftraggeber hat jeden Versand in eigenem Namen und unter eigenen Kennzeichen auszuführen. MAPP ist nicht verpflichtet, die Rechtskonformität des Versandes bzw. der zu versendenden Inhalte zu überprüfen. Der Auftraggeber sichert zu, ggf. erforderliche behördliche Erlaubnisse für die mittels des Services beworbene Dienstleistung bzw. das beworbene Produkt innezuhaben bzw. ggf. erforderliche behördliche Registrierungen vorgenommen zu haben.

5. DELIVERABILITY POLICY

- 5.1 Die Zustellbarkeit hängt von zahlreichen Faktoren ab. MAPP betreibt ein professionelles Deliverability Management und legt großen Wert auf modernste Technik, um eine Zustellbarkeit aller Nachrichten, welche über DMC gesendet werden, sicherzustellen. Dennoch erkennt der Auftraggeber an, dass die Zustellbarkeit von Nachrichten auch von Faktoren abhängt, die außerhalb der Kontrolle und des Einflusses von MAPP liegen und daher MAPP keine erfolgreiche Zustellung garantieren kann.
- 5.2 Die Zustellbarkeit von Nachrichten bzw. die Deliverability hängt zu einem großen Teil von der Qualität der Listen des Auftraggebers ab. Daher müssen diese Adresslisten den folgenden Anforderungen genügen:
 - a) Adressen, die von ihren Inhabern über einen längeren Zeitraum nicht mehr genutzt worden sind, werden von einigen Freemail-Providern zuerst gesperrt und senden dann für eine kurze Zeit (in der Regel ein Monat) eine Rejected Bounce-Nachricht. Anschließend werden einige dieser Adressen zu Spam-Traps umgewandelt, d. h. wenn diese Adressen weiterhin angeschrieben werden, wird die IP-Adresse des Absenders geblockt. Daher muss bei Adressen, die über DMC angeschrieben werden sollen, entweder die Einwilligung in den letzten zwei Monaten vor dem ersMappligen Versand über DMC erfolgt sein oder diese Adressen müssen regelmäßig, mindestens alle zwei Monate, angeschrieben worden sein.
 - b) Listen, die über DMC angeschrieben werden, müssen von Rejected Bounces bereinigt sein. Der Auftraggeber hat sicherzustellen, dass Adressen, welche Rejected Bounces auslösen regelmäßig (mindestens alle zwei Monate) blockiert

oder von der Liste vor dem ersten Versand gelöscht werden. Die Default-Einstellungen von DMC sehen eine automatische Sperrung von nicht-existierenden und dauerhaft deaktivierten Adressen nach dem ersten Rejected Bounce vor.

c) Ein Versand an eine bestimmte Liste darf eine Rate von 5 % Rejected Bounce nicht überschreiten. Die Rejected Bounce Rate wird berechnet anhand der Anzahl der Rejected Bounces im Verhältnis zum Gesamtvolumen eines Versandes. Wenn eine Liste mehr als 5 % solcher inaktiven Adressen enthält, ist davon auszugehen, dass die Liste über einen längeren Zeitraum nicht gepflegt wurde. Eine Rejected Bounce Rate von mehr als 10 % wird bei den meisten E-Mail- bzw. Freemail-Providern ("ISPs") zu einer Sperre bzw. einem Blacklisting der betroffenen IP-Adressen des Versenders führen.

d) Ein Versand an eine bestimmte Liste darf eine Rate von 3 % Spam Complaints nicht überschreiten. Die Spam Complaint Rate wird für jeden ISP, von dem MAPP die Mitteilungen über Spam Complaints erhält, individuell anhand der Anzahl der Spam Complaints im Verhältnis zum Gesamtvolumen des Versandes an den jeweiligen ISP berechnet. Eine Spam Complaint Rate von mehr als 3 % wird bei den meisten ISPs zu einer Sperre des betroffenen Versandes führen. Die Verpflichtung zur Bereinigung der Liste von Rejected Bounces aus dieser Ziffer 7 bleibt von dieser Regelung unberührt.

e) Listen müssen bestimmten Adressqualitätsstandards entsprechen und dürfen nicht mehr als 10 % (i) generische Adressen wie z. B. tech@domain.com, root@domain.com, (ii) so genannte „Wegwerf-Adressen“, die nur kurzzeitig gültig sind und insbesondere für die Teilnahme an Gewinnspielen verwendet werden (z. B. @mytrashmail.com oder @10minutemail.com); (iii) Adressen mit nicht-existent Domainkennungen (z. B. @lycos.de) (iv) technisch nicht mögliche E-Mail-Adressen z. B. E-Mail-Adressen ohne @) und (v) bei dem jeweiligen ISP nicht zugelassene E-Mail-Adressen (z. B. müssen E-Mail-Adressen bei einigen Providern mindestens vier Zeichen vor dem @ enthalten) enthalten.

f) Um die generelle Zustellbarkeit für alle Nutzer von DMC kontinuierlich weiter zu optimieren, ist MAPP berechtigt, aber nicht verpflichtet, Rejected Bounces einer universellen Bounce-Datei hinzuzufügen, um den Versand an Adressen zu verhindern, welche zuvor Rejected Bounces ausgelöst haben, indem die universelle Bounce-Datei als generelle Sperrdatei für alle Versendungen aus DMC verwendet wird.

6. LIST AUDIT UND KONSEQUENZEN

- 6.1 MAPP ist berechtigt, nach eigenem Ermessen eine Liste des Auftraggebers auf deren Adressqualität und Übereinstimmung hinsichtlich der Compliance und Deliverability Policy zu untersuchen. Auf MAPPs Anforderung hat der Auftraggeber detaillierte Informationen anzugeben, welche geeignet sind, die Einhaltung der Vorgaben der Compliance Policy zu belegen (z.B. Informationen über die Herkunft der Adressen und die vorhergehende Nutzung der Liste). MAPP darf dabei die Liste mit MAPPs universeller Bounce-Liste zu vergleichen, um Adressen zu identifizieren, welche Rejected Bounces auslösen können und somit die potentielle Bounce-Rate der Liste zu bestimmen.
- 6.2 Mit der Zustimmung des Auftraggebers kann MAPP Adresslisten des Auftraggebers einem Testversand unterziehen. Ein Testversand wird mit einer reduzierten Versandgeschwindigkeit (10.000 E-Mails/Stunde) an maximal 10% der Adressen der Liste (max. an 50.000 Adressen) durchgeführt.
- 6.3 Verstößt eine Versendung gegen die Compliance Policy und/oder die List Quality Standards, kann MAPP den jeweiligen Versand bei Kenntniserlangung von dem Verstoß unverzüglich stoppen. MAPP kann die von einem Verstoß betroffene Liste nach pflichtgemäßem Ermessen für weitere Versendungen über DMC sperren, wobei die Sperrung auf das erforderliche Maß beschränkt wird. Von einer Sperrung wird abgesehen bzw. eine Sperrung wird aufgehoben, wenn weitere Verstöße nicht zu befürchten sind. Eine Sperrung führt nicht zu einer Minderung der Vergütung.
- 6.4 Verstößt eine Versendung gegen die Compliance Policy und/oder die List Quality Standards, kann MAPP weitere Versendungen mit reduzierter Versandgeschwindigkeit (10.000 E-Mails/Stunde) durchführen, bis weitere Verstöße nicht mehr zu befürchten sind.
- 6.5 MAPP wird die Sperrung einer Liste aufheben, sobald weitere Verstöße gegen die Compliance Policy und/oder Deliverability Policy nicht mehr zu befürchten sind. Weitere Verstöße sind nicht zu befürchten, sobald der Auftraggeber nachvollziehbar dargelegt hat, wie weitere Verstöße verhindert werden. Diese Darlegung kann insbesondere auch durch die Beauftragung eines Deliverability Audits erfolgen. Ein Deliverability Audit ist eine detaillierte, kostenpflichtige Analyse und Reinigung von Adresslisten des Auftraggebers, um die Zustellbarkeit zu verbessern und die Einhaltung dieser Compliance und Deliverability Policy zu gewährleisten.
- 6.6 Bei wiederholten oder schwerwiegenden Verstößen gegen die Compliance Policy und/oder Deliverability Policy ist MAPP berechtigt, allerdings nicht verpflichtet, das DMC-System des Auftraggebers einem separaten IP-Pool mit geringerer IP Reputation zuzuordnen, bei dem eine Beeinträchtigung der Zustellbarkeit für die Versendungen des Auftraggebers nicht ausgeschlossen werden kann.
- 6.7 Wiederholte und/oder schwerwiegende Verstöße gegen die Compliance Policy und/oder Deliverability Policy werden als wesentliche Vertragsverletzungen gewertet
- 6.8 Die Parteien sind sich einig, dass der Auftraggeber allein verantwortlich ist für die Einhaltung dieser Compliance und Deliverability Policy, auch wenn MAPP ein List Audit durchführt und/oder einen Testversand durchführt und keine Listen des Auftraggebers sperrt und/oder die Sperrung einer Liste wieder aufhebt.