DIGITAL MARKETING ADDENDUM

1. SCOPE

This Digital Marketing Addendum shall apply to the usage of MAPP’s Software, especially, but not limited to, MAPP’s Digital Marketing Center (DMC), for purposes of digital marketing, especially, but not limited to, digital direct marketing via electronic messages and for Send-Outs in general. This Addendum should be read alongside the Agreement between the Customer and MAPP.

2. DEFINITIONS

2.1 “Address” means an email address, mobile number or any other electronic address information or facsimile number used to send Messages to via the Software.

2.2 “Business Day” means a working day other than Saturday, Sunday or public holiday at MAPP’s registered address.

2.3 “Deliverability” means the ability to deliver email messages in recipients’ inboxes and to avoid email messages being lost, blocked or driven to the spam folder.

2.4 “IP Address” means the internet protocol address, assigned to the mail servers used for Send-Outs.

2.5 “ISP” means email and web mail service providers like HoMappil, Gmail etc.

2.6 “List” means a list of Addresses used or intended to be used for Send-Outs via the Software.

2.7 “Message” means an electronic message (including, but not limited to email, SMS/MMS, push messages, in-app messages, instant messages and messages, posts and notifications on social media platforms) or a facsimile message.

2.8 “Personal Data” means any information relating to an identified or identifiable natural person as defined by the applicable data protection laws.

2.9 “Rejected Bounce” is the feedback information from an email server that the address an email was sent to does not exist or is permanently deactivated.

2.10 “Send-Out” means sending/broadcasting a Message via the Software.

2.11 “Spam Complaint” means the message by an ISP informing MAPP that an email sent via the Software has been marked as “junk“ or “spam“ by the recipient.

3. PROVISION AND USAGE OF DMC

3.1 Customer’s DMC system is provided under a subdomain delegated by Customer (e.g. news.customer.com). Customer shall delegate the subdomain to MAPP and provide all other information and cooperation required for the system setup at least five (5) Business Days prior to the scheduled system setup.

3.2 The transfer of data in a non-encrypted form can endanger the confidentiality of the data. Hence data transferred to MAPP for import into DMC must be transferred via a secure connection (e.g. sFTP). It is MAPP’s principle that the data provided by Customer is stored within the secure DMC environment only. For security reasons the data provided via FTP/sFTP servers is deleted from these servers on a regular basis.

3.3 Storage of information and reports regarding specific Send-Outs requires large storage capacities within the DMC environment. Information and reports are therefore archived 12 months after the specific Send-Out and are not directly accessible via DMC anymore. MAPP shall recover backups and archived information subject to charging its then current standard hourly rates. Pictures in and charts or attachments to Messages are deleted 6 months from the date of the Send-Out.

3.4 All data hosted and processed by MAPP on behalf of Customer is deleted from Customer’s DMC system immediately upon Customer’s request and upon termination of the Agreement. Deletion from the DMC system does not affect data in DMC system backups. In the event of termination of the Agreement Customer is required to download/export its data from its DMC system prior to the effective termination date. Upon termination Customer will no longer be able to access its DMC system. Customer is responsible for compliance with all retention obligations and requirements. MAPP is not under the obligation to store or hold records on behalf of Customer.

3.5 MAPP has the right to analyse Customer’s Send-Outs in an aggregated/anonymised form and to use these analyses for the maintenance and improvement of DMC and for statistical purposes, for market research and for publications (e.g. to determine the average opening rate of email newsletters in the FMCG sector). Customer will not be identified in such publications.

4. COMPLIANCE POLICY

4.1 Customer must comply with all applicable laws, regulations and industry best practice standards with respect to its usage of the Software including its processing of Personal Data via DMC, performing Send-outs via DMC and its usage of related services like hosting of websites/landing pages. Customer is responsible for the identification and interpretation of any applicable laws, regulations, and industry best practice standards that affect Customer's usage of DMC and MAPP's performance of Services for and/or on behalf of Customer. It is Customer's responsibility to assure compliance with any such requirements.

4.2 MAPP is not obliged to provide DMC to customers that perform Send-outs incompliant with applicable laws, regulations and industry best practice standards and/or to process such Send-Outs.

4.3 Commercial/marketing Messages as defined by the applicable laws, regulations and industry best practice standards may only be sent via DMC if the addressee consented to being sent the respective commercial/marketing Message or if the sending of the commercial/marketing Message is otherwise compliant with the applicable laws and regulations, in particular those that relate to data protection and fair trade and with the applicable industry best practice standards. The addressee's consent, if required, must comply with legal requirements with regard to form and content and be documented and verifiable in accordance with the applicable laws, regulations and industry best practice standards. The commercial character of commercial/marketing Messages must not be disguised or concealed.

4.4 Commercial/marketing Messages must contain Customer's contact information compliant with the applicable laws, regulations and industry best practice standards and must contain a unsubscribe link or other appropriate contact possibility for the recipients to revoke their consent and/or to unsubscribe from further commercial/marketing Messages. Unsubscribes submitted via the integrated DMC unsubscribe function will be processed automatically and the respective address will be blocked from future Send-Outs. Other unsubscribe processes provided by Customer must not be overly complicated. Unsubscribes received directly by Customer must be processed within (3) three working days. Customer must ensure that all messages to the "from address" and reply address indicated in the Message are processed immediately. Some ISP's inform MAPP if a Message sent via DMC is marked as "junk" or "spam" by the recipient (so-called "feedback loop"). DMC will treat such a marking as an unsubscribe and the respective Address will be blocked from further Send-Outs.

4.5 In the event that a Message sent by Customer (i) leads to a complaint by an addressee to MAPP, (ii) leads to a blacklisting by an anti-spam organisation (such as Spamhaus or Spamcop) or (iii) if MAPP receives a complaint or an inquiry by a supervisory or regulatory authority or any relevant association (such as direct marketing associations or consumer rights associations), Customer must, upon MAPP's first request and within one working day, provide evidence demonstrating the legality of the respective Send-Out. MAPP is entitled to disclose this evidence to third parties if necessary and to the extent required.

4.6 Customer must (i) not submit, save, link or otherwise indicate content that is pornographic, implicitly or explicitly sexually suggestive, threatening, insulting, harassing, defamatory, fraudulent, vulgar, obscene, hateful, left or right wing extremist or glorification of violence, or that invades personal rights, or contravenes the laws for the protection of young persons or calls for or abets infringement of laws, (ii) not submit, save, link, or otherwise indicate content that violates rights of third parties, including, but not limited to, trademark rights and rights to other signs, copyrights, patents, designs and utility models and trade secrets, and (iii) not submit, save, or link any malware (such as viruses) or otherwise indicate malware.

4.7 DMC offers numerous features and functionalities (such as campaign tracking, generating user profiles and behavioural or geographical targeting). The use of these features and functionalities may require the data subject's prior notification or consent. Customer must ensure that all features and functionalities are used in compliance with the applicable laws and regulations and with the applicable industry best practice standards. Customer must reconcile the Software's default settings with its specific requirements. It is Customer's obligation to register with and/or to obtain approval from the relevant authorities where required by the applicable laws and regulations.

4.8 Customer performs all Send-Outs in its own name, under its brand and nothing in a Message must indicate MAPP as the official sender of the Message. MAPP is not obliged and not able to monitor the compliance of Send-Outs with the applicable laws, regulations and industry best practice standards. Customer must hold any permits, licenses and permissions required for the services or products promoted via DMC.

5. DELIVERABILITY POLICY

5.1 Deliverability depends on numerous factors. MAPP operates a professional deliverability management and attaches great importance to its IP reputation. MAPP shall use commercially reasonable efforts and state-of-the-art technology to ensure deliverability of all Messages sent via DMC. Nevertheless, Customer accepts that the deliverability of Messages depends on factors that are beyond the control and influence of MAPP and that therefore MAPP shall not be responsible for successful delivery.

5.2 Deliverability depends to a great extent on the quality of Customers' Lists. Therefore Lists must meet the following requirements:

a) Addresses that have not been used by their holders for a long period are blocked by some ISP's who then send a rejected bounce message for a short time. Subsequently some of these Addresses are converted into spam traps and if such addresses continue to be written to the sender's IP Address or domain may be blocked. Therefore, Addresses that are intended to be written to via the Software require that either consent has been given in the last two months preceding the initial Send-Out or that these Addresses have been written to regularly, at least every two months.

b) Lists must be cleaned of Addresses causing Rejected Bounces. Customer must ensure that Addresses causing Rejected Bounces have been regularly blocked (every two months at least) or deleted from its Lists also prior to using the Software. The default settings of the Software provide for automatic blocking of Addresses having caused a Rejected Bounce after the first rejected bounce.

c) A Send-Out to a specific List must not exceed the rate of 5 % Rejected Bounces. The Rejected Bounce rate is determined by calculating the proportion of the number of Rejected Bounces to the total Send-Out volume to the List. If a list contains over 5 % of Addresses causing Rejected Bounces it must be assumed that the List has not been updated for a long period of time. With most ISP's a Rejected Bounce rate of over 10 % will lead to blocking or blacklisting of the sender's IP Addresses or domains concerned.

d) A Send-Out to a specific List must not exceed the rate of 3 % Spam Complaints. The Spam Complaint rate is determined individually for each (participating) ISP by calculating the proportion of the number of Spam Complaints received by a specific ISP to the total Send-Out volume to that ISP (both related to a specific Send-Out to a specific List). With most ISPs a Spam Complaint rate of over 3 % will lead to blocking or blacklisting of the sender's IP Addresses or domains concerned. The obligation to clean lists of Rejected Bounces in clause 5.6 remains unaffected.

e) Lists must meet specific address quality acceptance criteria and may not contain more than 10 % of (i) generic Addresses such as tech@domain.com, root@domain.com, (ii) so-called ‘‘disposable‘‘ Addresses, which are valid for a short time only and are used, inter alia, for participation in prize draws (such as @mytrashmail.com or @10minutemail.com), (iii) Addresses with non-existent domain names (such as @lycos.de), (iv) Addresses that are not technically possible (such as email addresses without @), and (v) Addresses that are not allowed at the relevant ISP (for instance, email addresses must contain at least (4) four characters before the @ sign with some ISPs).

5.3 To continuously optimise deliverability for all Customers, MAPP is entitled, but not obliged, to add Addresses causing Rejected Bounces to a General Bounce List and to prevent sending of Messages to Addresses that previously caused Rejected Bounces by using the General Bounce List as a general black list for all Send-Outs of all Customers.

6. LIST AUDIT AND NON-COMPLIANCE

6.1 MAPP is entitled to perform a List audit in order to test a List for its compliance with the Compliance Policy and/or Deliverability Policy at its own discretion. Upon MAPP's request Customer shall provide detailed information demonstrating the compliance of a List with the Compliance Policy (e.g. information on the source of the addresses and the previous usage of the List). MAPP may compare a List with the General Bounce List to identify addresses in the List that will cause Rejected Bounces and to thereby assess a List's potential Rejected Bounce rate.

6.2 With Customer's prior approval MAPP may conduct a test Send-Out to a List. Test Send-Outs are conducted with a reduced transmission speed (max. 10,000 emails per hour) to a maximum of 10 % of the Addresses of a List (but not exceeding 50,000 Addresses).

6.3 Any breach of the Compliance Policy and/or Deliverability Policy identified during a List audit or a test Send-Out or showing during or as a result of a regular Send-Out entitles, but does not oblige, MAPP to block further Send-Outs and to immediately stop on-going Send-Outs to the concerned List. The blocking will be limited to the necessary scope required to prevent further violations. A blocking shall not result in reduction of the fees. Recurring fees shall continue.

6.4 In case of breaches of the Compliance Policy and/or Deliverability Policy MAPP shall be entitled, but not obliged, to reduce the transmission speed for Send-Outs to the List (max. 10,000 emails per hour) alternatively to blocking the List.

6.5 MAPP lifts the blocking of a List or the reduction of the transmission speed if no further breaches of the Compliance Policy and/or Deliverability Policy are to be expected. Further breaches are not to be expected as soon as Customer has provided an explanation of what measures were taken to prevent further breaches (e.g. cleaning the List from Addresses causing Rejected Bounces). Customer can instruct MAPP to perform a Deliverability Audit. A Deliverability Audit is a detailed analysis and cleaning of a List intended to improve deliverability and ensure compliance with this Compliance and Deliverability Policy (available for a fee).

6.6 In case of repeated or serious breaches of the Compliance Policy and/or the Deliverability Policy MAPP is entitled, but not obliged, to assign Customer's system to a dedicated separate IP pool that may not provide the same high level of IP reputation as MAPP's general IP pool which may negatively impact the deliverability of Customer's Send-Outs.

6.7 A material and/or repeated breach of the Compliance Policy and/or the Deliverability Policy shall be considered a material breach of the Agreement.

6.8 For the avoidance of doubt, Customer shall remain solely responsible for its compliance with this Compliance and Deliverability Policy also/even if MAPP performs a List audit, Deliverability Audit and/or test Send-Out and does not block a List and/or lifts the blocking of a List.