CLOUD ADDENDUM

1. SCOPE

This Cloud Addendum applies to the provisioning of MAPP's Cloud Software and it should be read alongside the Agreement between the Customer and MAPP.

2. DEFINITIONS

2.1 "Cloud Software" means both SaaS and Hosted Software and excludes On-Premise Software.

2.2 "Data Controller" and "Data Processor" have the meaning as defined by the applicable data protection laws and regulations.

2.3 "Demarcation Point" means the point at which the public Internet connects to the MAPP border router.

2.4 "Financial Information" means all data related to bank accounts, credit and payment cards, credit ratings, account balances, and other monetary facts about a person or organization and especially includes all data subject to the Payment Card Industry Data Security Standard (PCI DSS).

2.5 "Force Majeure" means acts of God or government, civil commotion, military authority, war, riots, terrorism, strikes, fire, or other causes beyond the parties' reasonable control.

2.6 "Hosted Software" means a separate single-tenant instance of the Software, hosted and operated by MAPP and accessed by Customer remotely.

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

2.8 "SaaS" means "Software as a Service" and refers to a centralized instance of the Software serving multiple Customers, hosted and operated by MAPP and accessed by Customer remotely.

2.9 "Scheduled Maintenance" has the meaning as defined under Clause 3.3 below.

2.10 "Sensitive Data" means racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and Personal Data concerning health or sex life.

2.11 "Software" means any MAPP Marketing Applications standard software products licensed to Customer under the Agreement.

3. PROVISION OF CLOUD SOFTWARE

3.1 MAPP shall provide Cloud Software for Customer's usage in a secure system environment, hosted and operated by MAPP and accessed by Customer remotely. Cloud Software is not hired out to Customer. Usage of Software requires a standard browser according to MAPP's Supported Platform Matrixes (provided upon request). MAPP shall comply with all applicable laws and regulations applicable to MAPP with regard to operating and providing Cloud Software to Customer.

3.2 Usage of and access to Cloud Software will be limited as set out in the Agreement (e.g., available data storage space, processing power, number of concurrent users). Customer shall not exceed the limitations agreed to in the Agreement.

3.3 MAPP establish scheduled maintenance windows ("Scheduled Maintenance") to conduct routine maintenance during which time the Software may not be available. MAPP shall notify Customer of any Scheduled Maintenance reasonably (minimum 24 hours) in advance by email and/or via the MAPP At Your Service portal. MAPP shall use commercially reasonable efforts to perform Scheduled Maintenance outside the core business time (Monday to Friday 9am to 6pm). Scheduled Maintenance shall be limited to maximum 8 hours per calendar month.

3.4 Unless otherwise agreed upon in the Agreement, Customer is not entitled to an own IP address, an own physical server or a dedicated transmission capacity and bandwidth.

3.5 Customer acknowledges (i) that transmission of data over the Internet involves unique transmission risks that cannot be fully secure against access by third parties and Customer agrees that MAPP shall not be responsible for any loss or corruption of data which occurs during or as a result of transmitting data via the Internet; and (ii) that Cloud Software may be subject to intrusion through hacking and unauthorized use of Customer's logins and passwords, which are the sole responsibility of Customer.

3.6 MAPP performs system backups to ensure proper data processing on a regular basis in conformity with MAPP's then current backup procedures and policies (provided upon request), which MAPP may revise from time to time in its reasonable discretion.

3.7 MAPP leverages its global pool of experts and resources to provide the Products and Services under the Agreement to Customer. Customer acknowledges and agrees that the Software and any data (including Personal Data) residing within and/or processed by the Software may be transferred and hosted globally and/or accessed by MAPP globally from outside the national territory where the Customer and/or MAPP are located in order to perform MAPP's Services under the Agreement.

3.8 MAPP is entitled, but not obliged, to access the Software and to install and run diagnostic tools on the Software for purposes of (i) adjusting the settings of the Software in order to improve the performance and/or security of the Software, provided that these adjustments don't impair Customer's usage of the Software; (ii) collecting and storing usage and support related system data (not Personal Data) to aid in problem resolution and change control and to detect faults and to notify MAPP of such faults, (iii) generating statistical analysis; (iv) research and development.

4. USAGE OF CLOUD SOFTWARE

4.1 Customer must comply with all applicable laws, regulations and industry best practice standards with respect to its usage of the Cloud Software including its processing of Personal Data via the Cloud Software. Customer is responsible for the identification and interpretation of any applicable laws, regulations, and industry best practice standards that affect Customer's usage of the Cloud Software 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. Customer shall reconcile the default settings of the Cloud Software with its specific requirements.

4.2 Customer shall use the Cloud Software solely for its Internal Purposes and shall not (i) process infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including spam, material harmful to children or violative of third party privacy rights; (ii) process material containing software viruses, worms, trojan horses or other harmful computer code, files, scripts, agents or programs; (iii) knowingly interfere with or disrupt the integrity or performance of the Cloud Software; or (iv) attempt to gain unauthorized access to the Cloud Software or its related systems or networks. MAPP may remove any material or content that it reasonably believes violates this section upon notice to Customer.

4.3 Customer shall provide secure connectivity to access or transfer data to Cloud Software. In order to ensure confidentiality and integrity of Customer's data hosted/processed by the Software, Customer shall change login information upon receipt and shall keep login information strictly confidential. With regard to complexity and change periods Customer's login information shall conform to MAPP's current password policy requirements (provided upon request). Login information shall not be passed to any third party. Shared accounts are not permitted. Customer shall immediately inform MAPP in the event that login information was lost or compromised or if a specific login is no longer required.

4.4 Customer must not process Sensitive Data and/or Financial Information by the Cloud Software.

4.5 Customer shall backup all data made available to MAPP on a periodic basis commensurate with the risks.

4.6 Customer shall be solely responsible for:

a) any damage to Customer's data and/or the Software caused by the negligent or willful misconduct of Customer's employees, consultants or agents to whom Customer has provided access to the Software;

b) the conduct of any third party that has accessed the Software using Customer's passwords through no fault of MAPP;

c) Customer's failure to comply with all laws applicable to Customer's business;

d) having reasonable security processes, tools and controls for Customer's systems and networks interacting with the Cloud Software;

e) making its own elections regarding backup storage and alternative computing capabilities and business processes in the event that the Cloud Software is unavailable; and

f) determining the security, data protection and data backup facilities necessary for its business needs and its obligation or requirements to protect its data.

4.7 Customer shall ensure that MAPP's technical and organization measures and security controls fully meet its business needs and its obligation or requirements to protect its data.

5. AVAILABILITY

5.1 MAPP will use commercially reasonable efforts to make Cloud Software available 24 hours a day, 7 days a week. MAPP shall provide at least a Minimum Uptime Availability for its Cloud Software of 99 % during any calendar month.

Uptime Availability means that the connection between the servers on which the Cloud Software is hosted and MAPP's side of the Demarcation Point is uninterrupted and Customer is able to log in and access the cloud Software. The Minimum Uptime Availability does not refer to test and development servers.

5.2 MAPP measures the Uptime Availability of an availability test page within the Cloud Software at frequent intervals. The Uptime Availability percentage of the respective calendar month is calculated by dividing the number of successful availability measurements (test page available) by the total number of availability measurements of the respective calendar month, excluding Exclusion Times (as defined below). Uptime Availability measurement shall be carried out by MAPP and MAPP's measurement shall be relied upon by the parties and MAPP shall keep and shall send to the Customer, upon request, full records of its Uptime Availability measurement activities.

Exclusion Times are times during which the Cloud Software is unavailable due to:

- Scheduled Maintenance;
- Customer-caused or third party-caused outages or disruptions (except to the extent that such outages or disruptions are caused by third parties sub-contracted by MAPP to perform MAPP's contractual services) and/or
- outages or disruptions attributable in whole or in part to Force Majeure.

5.3 If the actual Uptime Availability percentage falls below the Minimum Uptime Availability in a given calendar month (Service Delivery Failure), Customer is entitled to a Service Credit. The Service Credit amounts to 1 % of the software license fees for the Cloud Software owed by the Customer for the affected calendar month for each 0,1 % by which the Uptime Availability percentage falls below the Minimum Uptime Availability. The Service Credit shall be limited to 25 % of the applicable fees of the affected calendar month. Service Credits shall be set off against subsequent invoices only, shall not be refunded to the Customer and shall lapse upon termination of the Agreement. A Service Credit shall not be credited unless the Customer requests it within two months of the end of the affected calendar month.

5.4 The Customer acknowledges and agrees that the terms of this Cloud Addendum relating to Service Credits in case of a Service Delivery Failure constitute a genuine pre-estimate of the loss or damage that the Customer would suffer as a result of the Service Delivery Failure, shall be Customer's exclusive remedy with respect to the Service Delivery Failure and are not intended to operate as a penalty for the Service Delivery Failure.

6. DATA PROTECTION

6.1 MAPP shall process Customer's data only in accordance with the terms of the Agreement and only on Customer's instruction. MAPP shall not process Customer's data for its own purposes. Customer shall always be and remain the Data Controller and MAPP shall be a Data Processor.

6.2 Customer and MAPP shall be separately responsible for conforming with such statutory data protection regulations as are applicable to them. Customer shall provide MAPP with such instructions as may reasonably be required by MAPP to fulfill its obligations under the Agreement. Customer acknowledges that MAPP is reliant on Customer for instructions as to the extent to which MAPP is entitled to process Customer's data. Consequently MAPP shall not be liable for any claim brought by a data subject from any act or omission by MAPP, to the extent that such act or omission resulted directly from Customer's instructions. Notwithstanding the foregoing, MAPP shall not be required to follow Customer's instructions if doing so would require additional Services or require MAPP to incur additional expenses, unless Customer has agreed to pay MAPP in respect of such fees.

Processing of Personal Data shall include such actions as specified in the Agreement. Within MAPP's area of responsibility, MAPP will have in place and maintain throughout the term of the Agreement the following technical and organizational measures to protect Customer Data against unauthorised or unlawful processing and/or accidental loss, destruction or damage:

- Prevention of unauthorised persons from gaining access to personal data processing systems (physical access control);
- Prevention of personal data processing systems from being used without authorisation (logical access control);
- Ensuring that persons entitled to use a personal data processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorisation (data access control);
- Ensuring that personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of

personal data by means of data transmission facilities can be established and verified (data transfer control);

- Ensuring the establishment of an audit trail to document whether and by whom personal data have been entered into, modified in, or removed from personal data processing systems (entry control);
- Ensuring that personal data processed are processed solely in accordance with the Controller's instructions (control of instructions),
- Ensuring that personal data are protected against accidental destruction or loss (availability control);
- Ensuring that personal data collected for different purposes can be processed separately (separation control).

Further details are available upon request. Customer shall be obliged to verify that the security measures taken are adequate for its individual protection requirements with regard to sensitivity, confidentiality and criticality of its data processed by MAPP.

6.3 Either party will inform the other as soon as practicable upon learning of a data breach on the Software involving Customer's data. The parties shall coordinate with each other to investigate the data breach and MAPP agrees to reasonably cooperate with Customer in Customer's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) facilitating interviews with MAPP's employees and others involved in the matter; and (iii) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable laws, regulations and industry standards. Each party will use best efforts to prevent a recurrence of any data breach as soon as practicable.

6.4 Upon Customer's written request (no more than once per calendar year), MAPP shall accurately complete a reasonable information security questionnaire provided by Customer regarding MAPP's data protection practices and policies and MAPP's information technology environment. After review of the questionnaire, Customer may make a written request at least 4 weeks in advance for an audit of the questionnaire responses. The audit shall take place over no more than 1 day during MAPP's normal business hours on a mutually agree schedule that will minimize the audit's impact on MAPP's operations. Customer may make no more than one audit every 2 calendar years unless an audit or questionnaire response reveals a breach of MAPP's obligations with regard to data protection under the Agreement. Customer and its auditors shall comply with MAPP's security requirements related to the performance of the audit.

6.5 If a governmental entity requests disclosure of Customer's data hosted by MAPP on behalf of the Customer, MAPP will try to redirect the government entity to the Customer first. If MAPP should nevertheless be required to respond to the request, MAPP will use reasonable efforts to notify the Customer in advance unless legally prohibited and MAPP will limit any disclosure of data to that data it is legally required to disclose.