Contract for the Commissioned Processing of Personal Data

between

Client name and address

("**Client**" / "**Controller**")

and

Emarsys Schweiz GmbH
Stauffacherstrasse 45
CH-8004 Zurich
Switzerland
("**Contractor**" / "**Processor**")

1. PREAMBLE

As part of a separate contract and/or on the basis of separate individual assignments (hereinafter collectively referred to as the "**Main Contract**"), the Contractor shall provide the Client with various marketing services, with particular emphasis on planning, implementing, and analyzing email communication (hereinafter collectively referred to as "**Services**"). The Services are described in more detail in the Main Contract and in the descriptions of each respective Service.

2. SUBJECT MATTER

2.1. Processing of personal data

This agreement ("**Contract**") shall provide regulations for processing personal data which the Contractor processes on behalf of Client whilst the Services are being delivered ("**Data**"). Personal data means any information relating to an identified or identifiable natural person. The Data particularly include the names, e-mail addresses, and areas of interest of the recipients of the Client's e-mail newsletters; further details regarding the type of personal data and categories of data subjects are set out in the Main Contract and the respective Service descriptions.

2.2. Extent of the commissioned data processing

The subject matter, duration, nature, and purpose of the processing of Data are set out in the Main Contract and the respective Service descriptions.

3. OBLIGATIONS OF THE CLIENT (CONTROLLER)

3.1. Client as controller

The Client remains the sole controller regarding the Data, and is responsible for the legality of the Data processing and protecting the rights of the data subjects. The Client shall inform the data subjects or obtain their consent with regards to the processing of Data where required.

3.2. Instructions

To the extent that Data processing is carried out by the Contractor using standard software, provided to the Client for online use, the Client shall usually exercise its authority to give instructions (see item 4.1) by utilizing the software's online interface. Other instructions from the Client are to be given using either the web interface provided to the Client by the Contractor, or in writing (including in electronic form); verbal instructions are to be confirmed in writing without undue delay. The Client reserves the right to give such instructions at any time. If the extent of the instructions received from the Client goes beyond what the Contractor is expected to carry out for the Client as per the Main Contract, the Client shall place an order and compensate the Contractor for the corresponding services separately.

3.3. Obligation to notify

If in the Client's area of accountability, Data which has been processed by the Contractor in accordance with this Contract becomes inadvertently known to unauthorized third parties, the Client shall inform the Contractor about this in due time to enable the Contractor to take necessary technical and organizational measures on its side.

3.4. Obligation to indemnify

If a third party (inclusive of public authorities) makes claim(s) against the Contractor and/or accuses the Contractor to be in breach of contract which is/are based on the Client's breach of its duties, the following shall apply: The Client shall grant the Contractor indemnity against these claims, provide the Contractor with appropriate support for their legal defense, and indemnify the Contractor for the reasonable cost of the legal defense. The obligation to indemnify shall only be valid if the Contractor informs the Client of any asserted claims in writing and without undue delay, does not make a confession or any other similar statement to that effect, and allows the Client, at the Client's own expense and as far as is procedurally possible, to conduct all legal and out of court proceedings regarding the claims.

4. DUTIES OF THE CONTRACTOR (PROCESSOR)

4.1. Requirement to observe instructions

The Contractor shall exclusively process the Data as part of, and for the purpose of, delivering Services for the Client and in accordance with the Client's documented instructions. The Contractor shall process the personal data in no other way, and for no other purpose, unless required to do so by EU or EU Member State law to which the Contractor is subject; in such a case, the Contractor shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2. Obligation to inform

The Contractor shall immediately inform the Client if, in its opinion, an instruction given by the Client violates applicable provisions in relation to data protection. The Contractor shall be entitled to suspend the performance of said instruction until it is confirmed or modified by the Client. The Contractor is not under any obligation to carry out a legal review of the instructions.

4.3. Obligation to Provide Support

The Contractor shall, upon the Client's request, adequately assist the Client in the event that the Client is only able to fulfil its obligations towards the data subjects (particularly the obligation to provide a data subject with details regarding the processing of his/her personal data) with the Contractor's assistance. The Contractor shall forward to the Client data subject requests directed to the Contractor. The Contractor shall also, upon the Client's request, assist the Client in ensuring its compliance regarding the security of personal data (security of processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject) as well as a potentially necessary data protection impact assessment and prior consultations, in each case taking into account the nature of processing and the information available to the Contractor. The Client shall place an order and compensate the Contractor separately for the

corresponding time and effort to the extent such support goes beyond the support required by applicable statutory law.

4.4. Rectifying, deleting, and blocking

Should personal data need to be rectified, deleted, or blocked, the Client shall undertake this themselves by using the corresponding functions available in the software provided. If this is not possible, the Contractor shall take on the tasks of rectifying, deleting, and blocking, following the instructions from the Client. Item 7.2 applies to the deletion of the Data at the end of the contract term.

4.5. Location of Data processing

The Data shall be processed solely in the European Union (EU) and/or in the member states which are included in the agreement covering the European Economic Area (EEA), provided that the Client has not permitted the Contractor to process the Data in a country outside of the EU and the EEA in this Contract or in any other manner.

4.6. Data protection officer

The Contractor shall have a designated data protection officer. The Contractor shall provide its data protection officer's contact details to the Client upon request.

4.7. Confidentiality of the Data

The Contractor shall familiarize its employees who are assigned with the task of processing personal data with the regulatory provisions of data protection, and shall commit them in writing to maintaining confidentiality and data secrecy. This obligation of secrecy especially applies to persons assigned with the task of processing data, and for data relating to legal bodies or an association, and shall continue to apply for the Contractor even after the employment is terminated.

4.8. Obligation to notify

If Client Data becomes known to unauthorized third parties in an unlawful manner, i.e. in breach of applicable data protection laws, this Contract, or instructions given by the Client, the Contractor must immediately inform the Client of this.

4.9. Technical and organizational measures

Taking into account the state of the technology, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of persons, the Contractor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Contractor shall, in particular, implement the technical and organizational measures specified in Annex 1 of this Contract in its area of accountability to ensure the security of processing. Furthermore, the Contractor shall take steps to ensure that any person acting under its authority who has access to the personal Data does not process it except on instructions from the Client, unless he or she is required to do so by EU or EU Member State law.

4.10. Insurance

The Contractor shall have appropriate insurance cover throughout the term of this Contract for possible liability claims arising from or in connection with this Contract.

4.11. Obligation to indemnify

If a third party (inclusive of public authorities) makes claim(s) against the Client and/or accuses the Client to be in breach of contract which is/are based on the Contractor's breach of its duties, the following shall apply: The Contractor shall grant the Client indemnity against these claims, provide the Client with appropriate support for their legal defense, and indemnify the Client for the reasonable cost of the legal defense. The obligation to indemnify shall only be valid if the Client informs the Contractor of any asserted claims in writing and without undue delay, does not make a confession or any other similar statement to that effect, and allows the Contractor, at the Contractor's own expense and as far as is procedurally possible, to conduct all legal and out of court proceedings regarding the claims.

5. THE CLIENT'S RIGHT TO CARRY OUT AUDITS

5.1. Certification

The Contractor must use an information security management system that is certified according to ISO 27001 during the term of this Contract, and shall provide proof of same upon request.

5.2. Audits

To the extent required, the Client is permitted to audit (or to have another auditor, mandated by the Client, audit) the Contractor's compliance with: a) the legal regulations in relation to data protection, b) the contractual agreements made by the parties and c) the Client's instructions. The Contractor shall contribute to such audits and make available to the Client all information necessary to demonstrate its compliance. The Client must give at least two weeks written notice prior to carrying out audits at the Contractor's business premises. The audits shall be carried out by the Client during the normal business hours, and without causing a significant disruption to business operations. Each party shall cover its own costs of, or in connection with, audits.

5.3. Legitimate interests of the Contractor

If by carrying out the audits the Contractor's trade and business secrets may be revealed, or intellectual property belonging to the Contractor could be compromised, the Client must have the audits carried out by an independent specialist third party which is under the obligation to maintain confidentiality with respect to the Contractor.

6. SUBCONTRACTING

6.1. Engaging subcontractors

The Contractor shall be authorized to engage subcontractors to process the Data if the Contractor enters into a written or electronic contract with the subcontractor regarding the processing of the Data, and the level of protection provided by said contract is equal or greater than that of this Contract, and the Client gives its prior written or electronic consent to engage the subcontractor. The Contractor shall inform the Client in writing or electronic form of any intended changes concerning the addition or replacement of subcontractors, thereby giving the Client the opportunity to object to such changes. The Client's consent shall be deemed given if the Client does not object in writing or electronic form within one month after receipt of this information.

6.2. Approved subcontractors

The Client hereby consents to engaging the subcontractors specified in Annex 2.

6.3. Liability for subcontractors

Where a subcontractor fails to fulfil its data protection obligations, the Contractor shall remain fully liable to the Client for the performance of that subcontractor's obligations.

7. TERM

7.1. Term

The term of this Contract shall correspond to the term of the Main Contract plus an additional 30 days. The right to termination for good cause shall remain unaffected.

7.2. Data at the point of contract termination

The Contractor shall delete the Client's Data from its data storage media and destroy any relevant documentation it holds, 30 days after the Main Contract has ended, provided that the Contractor is not legally obliged to continue storing it. The Client shall be responsible for exporting the Data in a timely manner before the end of this period, and to save it for its own continued use. The Client shall separately commission and remunerate the Contractor for Data that is published or exported in such a way that is not covered by the services included in the standard functions (e.g. downloading files).

7.3. Backup copies

The above obligation to delete shall not apply to copies of the Data which are included in regularly created back-up copies of the Contractor's comprehensive data sets, which would require the Contractor to invest significant resources to achieve an isolated deletion, and which will be automatically deleted or replaced after a maximum of 14 days as part of the back-up cycle that the Contractor applies. Until the automatic deletion or replacement occurs, any recovery or other use of such copies is prohibited after the termination of this Contract. The Client may request the Contractor delete such backup copies immediately if the Client reimburses the Contractor for the reasonable costs which are incurred by this; this also includes compensation for the incurred working hours of the Contractor's personnel.

8. FINAL PROVISIONS

8.1. Applicable Law

Exclusively Swiss law shall apply to this Contract (without possible references to other legal systems, and excluding the UN Convention on Contracts for the International Sale of Goods), provided that the Main Contract does not provide for the use of another applicable law.

8.2. Place of jurisdiction

Provided that the Main Contract does not specify otherwise, the place of jurisdiction for disputes resulting from or in connection with this Contract shall be Zurich, Switzerland.

8.3. Partial invalidity

In the event that individual provisions of this Contract are, or become, invalid, this shall not affect the validity of remaining provisions. A provision conveying the parties' original economic intention shall take the place of the invalid provision. The same shall apply to any unintended omissions in this Contract.

Client / Controller:		**Contractor / Processor:**	**Emarsys Schweiz GmbH**
Signature:		**Signature:**	
Name:		**Name:**	Hagai Hartman
Title:		**Title:**	General Manager
Date:		**Date:**	07.05.2018

ANNEX 1: TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE SECURITY OF PROCESSING

1. PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA

Measures which generally prevent unauthorized processing of personal data:

- Personal data are encrypted when transmitted.
- To the extent reasonably possible (without preventing the rendering of the agreed services) personal data are anonymized and/or pseudonymized by hashing or reference to a database whether personal data are stored.

2. ABILITY TO ENSURE THE ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

PHYSICAL ACCESS CONTROL

Measures which prevent unauthorized persons from gaining access to data processing systems which process or use personal data:

- Implementation of access prevention:
  - The area to be protected is secured using a suitable construction.
  - All possible manners of access are safeguarded against unauthorized access.
  - There is an access authentication system which is obligatory for all (key or smart card).
  - An access control system has been put in place.
- Management and documentation of personal access authorizations:
  - There are organizational regulations concerning access authorizations to operational areas.
  - There is documentation regarding the allocation of keys.
- Supervision of visitors and external staff:
  - There are guidelines for monitoring visitors and external staff (supervision, visitor pass, logging etc.).
  - There are regulations for monitoring maintenance staff (supervision, prior registration, checking identity etc.).

SYSTEM ACCESS CONTROL

Measures to prevent unauthorized persons from being able to use data processing systems (including encryption processes):

- Access protection (authentication):
  - User authentication is in place to protect access to data processing systems.
  - Checks are carried out to ensure the implementation of the measures protecting access.
  - A password generator is used to randomly generate passwords.
- Secured transmission of authentication credentials within the network:
  - Authentication credentials are encrypted when transmitted across the network.
- Blocking access in the event of failed login attempts/inactivity, and the process to reset blocked user IDs:
  - A secure resetting procedure is in place after access has been blocked, e.g. allocation of new user IDs.
- Prohibition on saving passwords and/or form entries on the local system:
  - Access passwords and/or form entries are not stored on the client or in its environment (e.g. saving in a browser or notes).
  - The users are given instructions about these requirements.
- Determining authorized persons:
  - A role concept is in place (predefined user profiles).
  - Access authorizations are always allocated on an individual (personal) basis.
  - The number of authorized persons is kept to the absolute minimum required for operation.
- Management and documentation of personal authentication devices and access authorizations:
  - A process for applying for, approving, allocating, and withdrawing authentication devices and access authorizations has been set up, described, and shall be used.
  - A person responsible for allocating access authorizations shall be specified.
  - Regulations on delegation are in place in case of the main person responsible being unavailable.
- Automatic access lock-out:
  - A password protected screen saver will be automatically activated by using the operating system's own built-in technology in the event of a workstation or a terminal remaining inactive for more than 30 minutes.
- Manual access lock-out:
  - Guidelines are in place to protect workstations and terminals against unauthorized use when the workplace is temporarily vacated, e.g. by automatic or manual activation of the password protected screen saver.
  - Employees shall receive training with regards to the necessity of using these measures.

DATA ACCESS CONTROL

Measures to ensure that persons authorized to use a data processing system have access only to the data they are authorized to access, and that personal data cannot be read, copied, altered, or removed without authorization during processing or utilization and after being saved (including encryption processes):

- Authorization concept/implementing access restrictions:
  - There are regulations regarding the creation, modification, and deletion of authorization profiles.
  - Each person authorized with access is only able to access the Data which he/she specifically requires to carry out the current process as per the processing methods agreed in this Contract, and which has been set up in the individual authorization profile.
  - If data sets including several Clients are saved in one database or are processed using the same data processing system, a logical access restriction method has been put in place to organize the processing of data for each respective Client (multi-client capability).
- Management and documentation of personal access authorizations:
  - A process for applying for, approving, allocating, and withdrawing access authentications has been set up.
  - Authentications are linked to a personal user ID and account.
  - If the basis for having an authorization is no longer in effect (e.g. in the event of a change of function), this authorization shall be withdrawn immediately.
- Logging of data access:
  - All operations relating to reading, entering, modifying, and deletion, are logged.
  - Regular assessments are carried out, on a random basis, to identify any possible misuse.

TRANSMISSION CONTROLS

Measures to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or transportation, or while being saved to data storage media, and that it is possible to ascertain and establish which areas personal data is to be transferred to using data transmission facilities (including encryption processes):

- Logging:
  - A log shall be kept of the sending and receiving areas.
  - The task is documented and made known to the affected employees.
- Secure data transmission between the server and client:
  - The data transmission between clients and servers is encrypted (SSL, SSH, SFTP, or VPN).
- Back-end transmission:
  - The connection to back-end systems is protected.
  - Data with high protection requirements is encrypted.
- Minimizing risk through network segmentation:
  - Network segmentation has been carried out with the aim of ensuring that the data transmission takes place over a minimum amount of network elements.
  - A network diagram has been created.
  - The relevant system is located in a DMZ.
- Security gateways to network transfer points:
  - Firewalls are in place at network transfer points.
  - The firewalls are always active.
  - The firewalls cannot be deactivated by the user.
- Hardening back-end systems:
  - Preinstalled service accounts/passwords have been deactivated.
  - Standard operating procedures are in place in the event of any suspicion of misuse.
  - Up-to-date anti-virus software is in place.
- Description of all interfaces and personal data fields to be transmitted:
  - There is a documented interface specification.
  - There are procedural requirements when transmitting.
  - There is a description of all personal data fields to be transmitted.
- Human-machine authentication:
  - Two-way authentication using cryptographic processes.
- Access to local cache:
  - All access to any local cache or databases which contain customer data from the Client for purposes and/or for use with applications that the Client has not authorized is denied using in-built technology.
- Personal data shall not be transmitted via the post.
- Process for collection and disposal:
  - There are regulations in place relating to the destruction of data storage media in a manner that is compliant with data protections laws.
  - There are regulations in place relating to the destruction of documents in a manner that is compliant with data protections laws.
- Deletion and destruction procedures according to data protection laws:
  - Data storage media must be wiped in accordance with data protection laws before being used by another user; recovering the deleted data is not possible, or only possible by investing a disproportionate amount of time and effort.
  - Hardware components or documents are to be destroyed in such a manner that recovering them is not possible, or only possible by investing a disproportionate amount of time and effort.

INPUT CONTROL

Measures to ensure that it is possible, after the activity, to check and ascertain whether personal data has been entered into, altered, or removed from data processing systems and if so, by whom (input control):

- There is documentation regarding which persons are authorized and responsible for entering, altering, or removing personal data in the data processing system, based on their assigned tasks.

INSPECTION OF COMPLIANCE DURING ASSIGNMENT

Measures to ensure that the commissioned personal data processing shall only be carried out in accordance with the instructions given by the Client (contract control):

- Only the Client is authorized to control assignments in the system.
- Exercising the obligation of inspection:
  - The Contractor shall support the Client when carrying out its obligation to inspect.
  - All incidents that occur shall be reported to the Client.
  - The Contractor shall inform all employees of their obligation to give information about incidents.
- Logging of the assignment execution by the Contractor:
  - There are records which ensure the complete traceability of the individual operational steps carried out as part of the assignment execution. Evidence can be provided upon request that the respective assignment has been carried out in strict accordance with the Client's instructions (minimum information: client/customer, action/partial order, exact specification of the process stages/parameters, authorized persons processing, dates, recipient if necessary).

3. ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT

AVAILABILITY INSPECTION

Measures to ensure that personal data is protected against accidental destruction or loss (availability inspection):

- Backup procedure:
  - There is a backup procedure in place.
  - Backups are carried out regularly.
  - A person and deputy responsible for the backup are specified.
  - Regular checks will be carried out to ascertain whether it is possible to restore a backup.
- Contingency plan:
  - A contingency plan is in place which details the steps to be taken and defines which persons, particularly on the Client's side, are to be informed of the incident.
- Testing the contingency arrangements:
  - Emergency power generators and overvoltage protection devices are regularly tested, and the operating parameters are under constant surveillance.

LIMITATIONS ON USE

Measures to ensure that data collected for different purposes can be processed separately.

- Data from the Contractor's different customers is to be saved in separate files and in separate directories, and is not to be merged together.

4. PROCESS FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING

ORGANIZATIONAL CONTROL

- Process definition/control:
  - There are procedural instructions.
  - Processes and operational procedures are defined for processing data in the company.
  - Checks are carried out on the implementation and compliance with processes.
- Training/obligation:
  - Principles of data protection, including technical and organizational measures.
  - Obligation to maintain confidentiality with regards to trade and business secrets, including the Client's procedures.
  - Handling data, files, storage media, and other documentation in due form and with great care.
  - Records of the training sessions are kept.
  - The training sessions shall regularly be repeated, at least once every three years.
- Training/obligation for external staff:
  - External staff shall only be given access to data processing systems and permitted to operate them once they have committed to, and have been trained on, data and telecommunications secrecy and other non-disclosure obligations.
- Internal allocation of duties:
  - Operative and administrative functions are kept separate.
- Substitute arrangement:
  - A substitute has been determined for all duties/functions critical for the operation of the business.

ANNEX 2: SUBCONTRACTORS

Subcontractor	Services rendered by the Subcontractor
Emarsys eMarketing Systems AG Märzstraße 1 1150 Vienna Austria	Development and provision of the marketing platform.
Emarsys Technologies Kft Kossuth Lajos utca 7-9 First Site Hotel & Business Complex Floor 2 1053 Budapest Hungary	Development and provision of the marketing platform.
Emarsys Interactive Services GmbH Stralauer Platz 34 10243 Berlin Germany	Agency services in relation to the planning, execution, and analysis of marketing communication.
Emarsys UK Ltd Focus Point 21 Caledonian Road London N1 9DX United Kingdom	Client support.
LINFORGE Technologies GmbH Brehmstraße 10 1110 Vienna Austria	Service partner for operational system administration.
CloudAMQP / 84codes AB Sveavägen 98 113 50 Stockholm Sweden	Message broker as a service.
CDNetworks Europe, Co. Ltd. 85 Gresham St London EC2V 7NQ United Kingdom	Content delivery network.
Heroku, Inc. The Landmark @ 1 Market St. Suite 300 San Francisco, CA 94105 USA	Platform as a service. All processing of personal data takes place within the European Union.
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Data storage engine. All processing of personal data takes place within the European Union.
Compose / IBM Corp. 1 New Orchard Road Armonk, New York 10504-1722 USA	Database as a service. All processing of personal data takes place within the European Union.