Data Processing Addendum in accordance with Art. 28 GDPR

1. Terms and Conditions.
This Data Processing Addendum ("Addendum") amends the Service Provider Agreement stipulated between the Parties defined in the Agreement. In the event of a conflict or inconsistency, the terms of this Addendum shall supersede those of the Agreement.

2. Subject matter and duration of the Processing
Vendor acting as Data Processor on behalf of Service Provider (Data Controller) collects, maintains and processes Personal Data and shall do so only for the purposes of the Agreement or as otherwise directed in writing by the Service Provider. In doing so, Vendor and Service Provider shall comply with the Data Privacy and Security requirements set forth in Annex 1 – Standard Contract Protections Concerning Data Privacy attached hereto.

Unless otherwise agreed in writing, the duration of the Processing corresponds to the duration of the Agreement.

3. Nature and purpose of the Processing

Nature and Purpose of Processing is further defined in the Agreement and respective service documentation.

4. Type of Personal Data and categories of Data Subject

The category of Data Subjects collected, processed and stored are:

- Customers (B2B)
- Employees of Customers and potential Customers (B2B)
- Subscribers
- Employees
- Contact Persons

The Personal Data processed by Vendor are:

- Personal Master Data (Key Personal Data)
- Contact Data
- Customer History
- Contract Billing and Payments Data

Annex 1 - Standard Contract Protections concerning Data Privacy

1. Data Privacy

1.1 In this Addendum the following terms shall have the meanings set out below:

(a) "Data Subject" means a natural person whose Personal Data is Processed;

(b) "Data Protection Legislation" means laws and regulations, which protect the privacy rights of individuals, in so far as those laws and regulations apply to the Processing of Personal Data in connection with this Agreement, including without limitation Data protection legislation enacted by Switzerland, the EU and EU Member States, and similar measures;

(c) "Data Security Breach" means as is defined in Section 2.2 (c) below;

(d) "Personal Data" means any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(e) "Sensitive Data" means Personal Data revealing racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation, etc.;

(f) "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(g) "Data Controller" means the entity disclosing the Personal Data, i.e. Service Provider;

(h) "Data Processor" means the entity receiving the Personal Data, i.e. Vendor;

(i) "Data Protection Impact Assessment" means an analysis of how Personal Data is collected, used, shared, protected and maintained.

1.2 Service Provider shall in its quality of Data Controller:

(a) Inform Data Subjects of its rights;

(b) Inform Data Subjects of the Personal Data collected in the context of Vendor;

(c) Ensure that there is a legal basis to Process Personal Data and, if the legal basis is consent of Data Subjects, collect and log the consent of Data Subjects associated to the collection, storage and Processing of its Personal Data;

(d) Ensure that no Sensitive Data is uploaded into Vendor solution;

(e) Communicate to Vendor the contact details of the security officer(s) and data protection officer(s).

The Service Provider warrants towards Vendor that any Personal Data disclosed to Vendor was collected in a lawful way and does not infringe upon the rights and freedoms of the Data Subject and/or third parties.

The Service Provider will sign a DAP agreement with the client where appropriate and as such pass on the responsibilities of 1.2 (a – e) to the Data Controller the Customer in the scope of this agreement.

1.3 Vendor shall:

(a) Use all reasonable endeavors to assist Service Provider in its compliance with Data Protection Legislation, including without limitation the preparation of necessary notifications, registrations and documentation which Service Provider may be reasonably required to make or enter into in order to comply with Data Protection Legislation in connection with this Agreement;

(b) Only process the Personal Data in accordance with Service Provider's documented written instructions, which may be specific instructions or standing instructions of general application in relation to the performance of Vendor obligations under the Agreement, unless otherwise required by applicable law to which Vendor is subject. In such a case, Vendor shall inform Service Provider of that legal requirement before carrying out the required Processing, unless that law prohibits such information on important public interest grounds;

(c) Put in place measures to ensure:

that any employees who have access to Personal Data do not process the Personal Data except on instructions from the Service Provider, unless required to do so by applicable law to which Vendor is subject; and

that any employees who have access to Personal Data are reliable and have committed themselves to confidentiality;

(d) Not disclose the Personal Data to any other body (including any subcontractor) without Service Provider's express agreement in writing;

(e) Not transfer Personal Data from the European Economic Area or relating to residents of the European Economic Area to any location outside Switzerland or the European Economic Area unless:

Service Provider has consented to such transfer and such transfer complies and continues to comply with the requirements for international data transfers under applicable Data Protection Legislation or;

if the specific Conditions of Article 44 et seq. GDPR (and/or similar provisions under other applicable Data Protection Legislation) have been fulfilled.

(f) Commission subcontractors (additional contract processors) only after prior specific or general written or documented consent of Service Provider.

Service Provider agrees to the commissioning of the list of subcontractors attached to this Addendum as Annex 2, on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR;

Further outsourcing to subcontractors or changing of existing subcontractors are permissible if (1) Vendor submits such an outsourcing to a subcontractor to Service Provider in writing or in text form with appropriate advance notice; (2) Service Provider has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to Vendor; and (3) The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(g) Promptly notify Service Provider if Vendor receives a request from a Data Subject to have access to Personal Data or exercise any other applicable Data Subject rights, and assist the Service Provider insofar as reasonably possible in responding to any such complaint or request, including, without limitation:

where authorized by Service Provider, by allowing the Data Subject to have access to its Personal Data or to have that Personal Data corrected, deleted, or blocked within the relevant time frames set out by applicable law;

by providing the Service Provider with any requested information relating to the Processing of Personal Data under this Addendum;

by providing the Service Provider with any Personal Data Vendor holds in relation to a Data Subject, if required in a commonly-used, structured, electronic and machine-readable format;

(h) If Service Provider is obliged by Data Protection Legislation to carry out a Data Protection Impact Assessment in relation to the services Vendor provides pursuant to this Agreement Vendor will provide the Service Provider with such support and information as reasonably required in carrying out such assessment;

(i) Permit Service Provider (or the duly authorized representatives or any regulator to which Service Provider is subject) to inspect and audit Vendor Processing activities under this Agreement (and/or those of any of its agents or subcontractors to whom Vendor has been permitted by Service Provider to disclose the Personal Data), and comply with all reasonable requests or directions by Service Provider to enable them to verify and/or procure that Vendor is in full compliance with the obligations under this Agreement;

Vendor may claim a reasonable compensation for all costs such an inspection or audit may involve.

(j) Immediately inform Service Provider if in Vendor's opinion one of the Service Provider's instructions infringes the provisions of applicable Data Protection Legislation;

(k) If so requested by Service Provider at any time, provide them with a copy of the Personal Data or (at Service Provider's option) destroy it; and;

(l) Upon termination of Vendor provision of services relating to Personal Data, delete or return all the Personal Data to Service Provider and delete any existing copies of the Personal Data, save where applicable law requires Vendor to retain copies of such data.

2. Security

2.1 Service Provider is responsible for the proper creation and management of its user accounts, including user account disabling and account reviews. Service Provider mainly must ensure that:

(a) Access and authorizations are granted on the need to have;

(b) Each individual is assigned with a unique account;

(c) Accounts are periodically reviewed to validate their relevance;

(d) Generic accounts are not used;

(e) Passwords contain at least 8 characters consisting in a combination of characters, numbers and symbols;

(f) Passwords lifespan does not exceed 90 days;

(g) Suspected compromised accounts are disabled at once.

2.2 Vendor must:

(a) Implement and maintain appropriate technical and organizational measures to ensure the security and protection of Personal Data, taking into account the nature and sensitivity of the information to be protected, the risk presented by Processing, the state of the art, and the costs of implementation, in compliance with applicable Data Protection Legislation. Such measures shall include appropriate physical, electronic and procedural safeguards, to (1) ensure the security and confidentiality of Personal Data, (2) protect against any threats or hazards to the security or integrity of Personal Data, and (3) prevent unauthorized access to or use of Personal Data, without limiting any other obligations under this Agreement;

(b) Keep in force the security measures set forth in Technical and Organizational Measures provided in annex to this Addendum.

(c) Notify the Service Provider as soon as reasonably possible if they know, discover or reasonably believe that there has been (1) any unauthorized access to or acquisition of Personal Data that compromises the security, confidentiality or integrity of Personal Data, or (2) any unauthorized disclosure of, access to or use of any Personal Data, or (3) any unauthorized intrusion into systems containing Personal Data resulting in unauthorized access or access in excess of authorization ("Data Security Breach");

(d) In the event of a Data Security Breach, (1) immediately investigate, correct, mitigate, remediate and otherwise handle the Data Security Breach, including without limitation, by identifying Personal Data affected by the Data Security Breach and taking sufficient steps to prevent the continuation and recurrence of the Data Security Breach; and (2) provide information and assistance needed to enable the Service Provider to evaluate the Data Security Breach and, if applicable, to provide timely notices disclosing a Data Security Breach and to comply with any obligations to provide information that the Data Security Breach to relevant regulators;

3. Liability

3.1 The provisions on liability of the Agreement apply.

3.2 Service Provider shall indemnify Vendor in its sphere of responsibility from any and all claims brought against Vendor by a person in accordance with Art. 82 para 1 GDPR. Insofar as Service Provider is obliged to pay compensation to such persons due to Vendor's fault, Service Provider reserves recourse against Vendor.

3.3 Vendor shall indemnify Service Provider in its sphere of responsibility from any and all claims brought against Service Provider by a person in accordance with Art. 82 para 1 GDPR due to the fact that Vendor infringed upon obligations under the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instruction of Service Provider. Insofar as Vendor is obliged to pay compensation to such persons due to Service Provider's fault, Vendor reserves recourse against Service Provider.

3.4 If a Party (uninvolved Party) has to pay an administrative fine in accordance with Art. 83 GDPR due to misconduct of the respective other Party (misconducting Party), the misconducting Party shall fully indemnify the uninvolved Party from such administrative fines as well as all reasonable cost of legal representation in this regard.

3.5 The limitations of liability as agreed in the Agreement apply.