Agreement on Processing on Behalf

regarding the main agreement ("Main Agreement") between the customer ("Controller") and QENTA Payment CEE GmbH (QENTA Payment CEE) ("Processor"):

§1 Subject Matter and Duration of Processing on Behalf

(1) Once the respective Main Agreement between the customer (Controller) and QENTA Payment CEE (Processor) is signed, this data processing agreement on behalf ("Agreement") shall become an integral part thereof.

(2) This Agreement specifies the statutory rights and obligations resulting for the Controller and the Processor from applicable data protection legislation, in particular from the General Data Protection Regulation /Regulation (EU) 2016/679), in the following referred to as "GDPR"), as well as the applicable national implementing legislation, if and as far as the Processor processes personal data for the Controller within the scope of the Main Agreement.

(3) The subject matter and purpose of processing on behalf of the Controller ("Processing") shall be the processing of electronic payment transactions as well as identity verification, fraud checks, anti-money-laundering prevention, risk management assessments and solvency assessments, to the extent the Controller has instructed the Processor with these tasks in the Main Agreement.

(4) The duration of Processing shall comprise the term of the Main Agreement within the framework of which this Agreement has been concluded.

§2 Contents of the Agreement

(1) The scope, nature and purpose of the intended collection, processing and use of data shall include
(a) fulfilment of the Processor's obligations resulting from the Main Agreement;
(b) collection from the data subject or from the Controller through online completion for the initiation, authorisation, implementation and processing of payment transactions in connection with the ordering of goods or services on the Internet, via telephone or telefax;
(c) transfer of this information to the operator of the type of payment selected by the end customer for the respective transaction;
(d) inquiries to financial information service providers for risk management assessments as well as solvency assessments within the scope of the initiation and implementation of the business relationship as well as fraud prevention, to the extent the Controller so has instructed the Processor in the Main Agreement

(2) The categories of data shall include
(a) Information about the end customer of the Controller (e.g. first and last name, address, email address, date of birth, IP address)
(b) Information on the chosen type of payment as well as payment information of the end customer (e.g. credit card and bank account information)
(c) Information on the transaction (e.g. goods, article numbers, purchase price and similar information)
(d) Information on the current and on past transactions of the end customer with the Controller and with other merchants with which the Processor cooperates (e.g. about chosen products and types of payments) if a solvency assessment is carried out
(e) Solvency information collected from financial information services providers that allow conclusions about the end customer's solvency (e.g. final claims against the end customer) to the extent this information is necessary for fulfilment of the above referenced purposes.

(3) The data subjects are the Controller's end customers.

§3 Technical and Organisational Measures

(1) To ensure that the Processing governed by the agreement specified above in the form concluded between the parties will be properly implemented by the Processor, the Processor has taken appropriate technical and organisational measures for data security within the meaning of Articles 28, 32 GDPR. The Appendix to this Agreement provides the Controller with an overview of the measures taken as of the date on which this Agreement is concluded.

(2) The technical and organisational measures are subject to technical progress and further developments. In this respect, the Processor shall be permitted to further develop any measures taken and/or to replace them by adequate alternatives. In doing so, the degree of protection must not drop below the level of data protection prescribed by statute. Any significant changes shall be documented. The Processor will provide the Controller with information on the applied technical and organisational measures at any time upon request.

§4 Rectification, Blocking and Deletion of Data

The Processor shall support, within its possibilities, the Controller upon the Controller's instructions in its obligation to respond to requests for exercising the data subjects' rights pursuant to Chapter III GDPR and will implement the suitable and necessary technical and organisational measures. To the extent that any data subject directly addresses the Processor for the purpose of having his/her personal data rectified or erased, the Processor shall forward this request to the Controller. To the extent that the Processor supports the Controller in meeting the requirements of any data subjects, the Controller shall reimburse the Processor for the costs and expenses incurred.

§5 Obligations of the Processor

(1) The Processor will process (including transfer) the personal data only upon instruction, i.e. the Controller's documented order instructing a specific handling of data by the Processor relevant under data protection laws (e.g. anonymization, blocking, deletion, submission), unless it is statutorily obliged to processing; in this case it will inform the Controller of this statutory requirement in advance, unless such information is prohibited based on an important public interest.

(2) The Processor warrants that the employees used by the Processor for data processing purposes have been obliged in writing to observe data secrecy in accordance with Article 28 para 3b) GDPR or are subject to appropriate statutory confidentiality. To the extent that the Controller is subject to any further confidentiality obligations, for example in accordance with any regulations under professional law, criminal law or procedural law, the Controller shall inform the Processor thereof and shall, upon request, educate the Processor and the latter's employees on the application of the confidentiality obligations.

(3) The technical and organisational measures, as defined in clause 3 of this Agreement and the corresponding appendix, are implemented and complied with by the Processor. This includes in particular
(a) Pseudonymisation and encryption of personal data
(b) The ability to ensure, on a continuous basis, confidentiality, integrity, availability and reliability of the systems and services in relation to the processing of personal data;
(c) The ability to ensure availability of personal data and access to the data in case of a physical or technical accident;
(d) A procedure for regular inspection, assessment and evaluation of the efficacy of the technical and organisational measures for ensuring the security of processing.

(4) To the extent that no conflicting procedural considerations exist, the Processor shall inform the Controller of any regulatory measures of the competent supervisory authority in accordance with Art 58 GDPR as well as on any court decisions in connection with Articles 83, 84 GDPR.

(5) The Processor appointed a data protection officer (cf. § 12).

(6) The Processor shall be obliged to provide the Controller with information at any time to the extent that this affects the personal data and documents transferred by the Processor. Any data that is no longer required shall be erased at Processor without undue delay in accordance with clause 4 of this Agreement. Any controls that extend beyond this Agreement shall be governed exclusively by the statutory regulations.

§ 6 Support pursuant to Art 32 – 36 GDPR

Upon request, the Processor shall support the Controller, within reason and taking into consideration the type of processing and the information available to it, in the Controller's compliance with its obligations pursuant to Art. 32 to 36 GDPR with appropriate technical and organisational measures. This concerns, inter alia, the data subjects' rights, security of processing, notification of breaches and respective information to the data subjects, support in case of inspections by a data protection authority, and in data protection impact assessments. The Controller will reimburse the Processor for all costs and expenses incurred in relation with this, unless the measures causing the costs/expenses were caused by the Processor. If the parties cannot agree on the extent of reimbursement, all costs and expenses that the Processor may have deemed necessary will be reimbursed in full.

§7 Establishment of Sub-Processing Relationships

(1) To render the contractual services, the Processor may award parts of the Processing to subcontractors. The following subcontractors has been instructed to render services relevant to the Agreement as of the date of conclusion of the Agreement: In the event of any credit card payment processing, services will additionally be rendered by:
(a) QENTA Payment CEE GmbH, Germany
The Controller agrees to the subcontracting to the aforementioned companies. The Controller also agrees to the subcontracting to further companies provided the obligations of this Agreement are forwarded to the subprocessors and at least the same level of protection will be maintained.

(2) In case of any involvement of any further subcontractors, the Processor shall inform the Controller. In addition, the Controller may reject additional subcontractors of the Processor only if there is any compelling reason under data protection law to do so and this has been communicated to the Processor in writing immediately after the information had been received. Subcontractual relationships within the meaning of this provision shall not be deemed to include any such services of which use is made by the Processor from any third parties as an ancillary service for support in the implementation of the Agreement. This shall include, inter alia, telecommunication services including housing, as well as any transfer and hosting of data, transport and communication services, cleaning staff, as well as any disposal of data carriers and documents.

(3) Within the framework of the subcontractual relationships, the Processor shall enter into any agreements required under data protection law. The Processor is permitted to process the data also outside of the EEA in compliance with the provisions of this Agreement, or to have them processed, provided that it informs the Controller in advance on the location of the data processing an evidences compliance with the technical and organisational measures. This section 7 shall fully apply to any subcontractors. The Controller hereby authorises the Processor to enter into any agreements with subcontractors, in representation of the Controller – including, but not limited to, (sub)processing agreements and EU Standard Contractual Clauses or similar agreements – that are required to guarantee an appropriate level of data protection with regard to the transfer of data. The Processor may grant subcontractors substitute powers of attorney. The Controller agrees to provide support in meeting the legal requirements of the transfer of data.

§8 Controller's Rights to Monitor

(1) The Controller shall convince itself that its personal data is properly processed and that the technical and organisational data security measures taken at the Processor's premises on site are complied with. To this end, the Processor shall, upon the Controller's request, demonstrate compliance with the technical and organisational measures by means of uptodate certificates, reports or extract of reports of independent entities (such as internal audit, data protection officer, IT security department, external data protection auditors) or any certification by an IT security or data protection audit (e.g. in accordance with PCI DSS) and/or acknowledged certifications pursuant to ISO 27001.

(2) The Processor shall enable and support the Controller or an external independent auditor instructed by the Controller, the review, including inspection, in particular if there was a security incident and/or a review, including inspection, is requested by the legislator or a data protection authority. The Controller or its instructed independent third party may access the premises of the Processor at which data pf the Controller are processed, after respective notice and during normal business hours, at its own cost and without interruption to the business operations, ensuring the secrecy of any trade or business secrets of the Processor and any potential subcontractors, to convince itself of compliance with the technical and organisational measures of Appendix 1.

(3) The Controller shall inform the Processor sufficiently in advance (usually at least four weeks) about all circumstances in relation to the carrying out of an inspection. The Controller may, as a rule, carry out one inspection per calendar year. This shall not affect the Controller's right to conduct further inspections in case of violations of data protection obligations of the Processor.

(4) If the Controller instructs a third party with the inspection, the Controller shall oblige this third party in the same way as the Controller is obliged to the Processor under this Agreement. Upon request the Controller must provide the respective agreement with such third party to the Processor. The Controller must not instruct a competitor of the Processor with an inspection.

(5) The Processor is permitted, in its own discretion and taking into account the statutory obligations of the Controller, to not disclose information that is sensitive with regard to the Processor's business or if the Processor would breach statutory or contractual obligations with the disclosure. In particular, the Controller will not receive access to information about other business partners of the Processor as well as about any other nonpublic information of the Processor that is not strictly required for the statutory inspection rights.

(6) The Controller will reimburse the Processor for its costs and expenses in relation to the evidencing of compliance with the technical and organisational measures, in particular the expenses in relation to any reviews and inspections on its premises.

§9 Notification in Case of Infringements by the Processor

The Processor shall promptly inform the Controller if it becomes aware of a breach of the protection of personal data of the Controller. The Processor shall take the measures necessary to safeguard the data as well as to minimise any potential adverse consequences for any data subjects in coordination with the Controller.

§10 Controller's Responsibility and Authority to Issue Instructions

(1) The Controller shall be the controller for the processing of data on behalf by the Processor. The evaluation of the admissibility of the data processing shall be the obligation of the Controller. The Controller shall provide the Processor with the data in due time and in the required quality to ensure that the Processor will be able to render the services.

(2) The Processor shall process the personal data provided to it within the framework of the instructions issued by the Controller as stipulated in the Agreement.

(3) The Processor and its subcontractors may process the data for their own purposes in accordance with data protection law, provided that this is permitted by statute or the data subject's consent. This Agreement shall not be applicable to any such data processing. In any case, the Processor and its subcontractors may process the data for their own purposes in an anonymised form.

(4) The Controller shall bear additional costs incurred due to any instructions; the Processor may request an advance payment. The Processor may refuse to carry out any additional or modified data processing if it would result in any change in the amount of work or if the Controller refuses to reimburse the additional costs or to make the advance payment.

(5) For reasons of traceability, any instructions of the Controller shall be given in writing or in text form (e.g. by email); any oral instruction shall be confirmed in writing or in text form without undue delay.

(6) If the Processor considers that an instruction given by the Controller infringes the GDPR, the Austrian Data Protection Act or any other data protection regulations, the Processor may refuse to execute the instructions until the Controller has confirmed the instruction or has changed it into an instruction that is in accordance with data protection regulations.

§11 Deletion of Data and Return of Storage Media

Upon the end of the contractual relationship, the Processor shall be obliged, at the Controller's option, to delete, to block or to return to the Controller any personal data that has been provided to the Processor in connection with the service agreement and has not yet been deleted by then. Any retention obligations, including but not limited to those in accordance with statutes, bylaws, contracts and regulatory instructions, shall remain unaffected.

§12 Point of Contact for Data Processing and Data Protection Queries

On the part of the Controller:

The data protection officer of QENTA Payment CEE can be reached under privacy@qenta.com

§13 Final Provisions

(1) This Agreement shall become an integral part of the Main Agreement.
(2) This Agreement includes any and all agreements with respect to its subject and shall in this respect replace all previous agreements between the Controller and Processor.
(3) Unless set forth otherwise above, the current version of the General Terms and Conditions of QENTA Payment CEE applicable to the Main Agreement shall be applied to the Agreement. This shall apply especially to the application of jurisdiction, applicable law, interpretation, severability and the obligatory written form clause to these provisions. In the event of contradictions, the provisions of this Agreement take precedence over all other contractual agreements and the General Terms and Conditions of QENTA Payment CEE.