Data Processing Agreement

This data processing agreement (hereinafter "**Agreement**") reflects an agreement with respect to the terms governing the processing of the personal data transferred to BaseinGO OÜ, registry code **16440184**, address Ahtri tn 12., Tallinn 10151 (hereinafter "**Processor**") by its customer during the provision of Service.

The term "**Customer**" refers to a legal entity which has been founded during the course of Service Agreement signed between the Processor and natural person as a founder of the Customer (hereinafter "**Freelancer**") and further accepted by the Customer. Customer's acceptance to the Service Agreement and this Agreement shall form a legally binding agreement between the Customer and Processor.
The Processor and the Customer jointly referred to as the "**Parties**" and each separately as the "**Party**", HAVE AGREED on the following terms in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer of the personal data specified in Appendix 1;

1 DEFINITIONS

1.1 "**Data Subject**" means an identified or directly or indirectly identifiable natural person.

1.2 "**Personal Data**" means any information relating to a Data Subject.

1.3 "**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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.4 "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. Within the meaning of this Agreement, the Customer is considered as Controller.

1.5 "**Subprocessor**" means a third party data processor engaged by the Processor, who has access to or processes Personal Data at the request of the Processor. Processor may engage different types of Sub-processors to perform various functions.

1.6 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.7 "**Service**" means any services provided to the Customer after it has been founded as a legal entity and during which the Processor may become aware of Data Subjects and their Personal Data which the Customer is processing in its business activity.

2 OBJECT OF THE AGREEMENT

2.1 The Parties undertake to comply with all obligations arising from any applicable data protection legislation, including but not limited to the EU General Data Protection Regulation no 2016/679 and the Estonian Personal Data Protection Act.

2.2 The Parties shall refrain from any action, which could result in the other Party's failure to comply with its obligations under the applicable data protection legislation.

2.3 During the provision of Service the Processor may be required to process Personal Data on behalf of the Customer. By this Agreement, the Parties shall agree on Personal Data Processing requirements in order to secure that the Processing complies with the respective data protection law and to ensure the protection of Data Subject's rights.

2.4 Under this Agreement, the Customer is acting as data controller and the Processor is acting as a data processor in the meaning of General Data Protection Regulation.

3 GUARANTEES FOR PERSONAL DATA PROCESSING

3.1 Processor shall process the Personal Data only to the extent, and in such a manner, as necessary for the provision of Service.

3.2 Processor confirms that it shall not process the Personal Data for any other purpose which is not specified in the Appendix 1 of this Agreement. To ensure this the Processor shall:

3.2.1 refrain from any personal use, including commercial use, of the Personal Data processed for the provision of Service;

3.2.2 comply and ensure that its own employees or any third parties used by the Processor comply with the principles of the applicable data protection regulation, incl. comply with confidentiality clause; and

3.2.3 provide the Customer with all necessary information to demonstrate that it complies with this Agreement; and

3.2.4 process the Personal Data only on behalf of the Customer and in compliance with its instructions and the Agreement.

3.3 If the Processor cannot provide compliance for whatever reasons, it agrees to inform promptly the Customer of its inability to comply, in which case the Customer is entitled to suspend the transfer of data and/or terminate the Agreement.

3.4 Processor shall promptly notify the Customer about:

3.4.1 any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

3.4.2 any accidental or unauthorised access;

3.4.3 any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so.

3.5 The Controller grants the Processor a general authorization to subcontract Processing of Data Subject's Personal Data under this DPA to Subprocessors, provided that:

3.5.1 the engagement of the Subprocessor is necessary for the provision of the Service;

3.5.2 the Processor has entered into a written agreement containing data protection obligations no less protective than those in this Agreement. The Processor shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

3.5.3 the Processor will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to establishing that it is capable of providing the level of protection of Personal Data required by this Agreement.

3.6 Processor will make the list of Subprocessors, incl. the role of each subprocessor, in place on the effective date of the Agreement, available to the Controller upon request.

3.7 If the Processor wishes to amend criteria established under the general authorization set forth in this paragraph, then the Processor shall notify the Controller by e-mail. The Controller's continued use of

the Processor's Service after such notice shall constitute the Controller's consent to the new criteria, unless the Controller objects pursuant to the clause below.

3.8 The Controller may reasonably object by notifying the Processor in writing within fifteen (15) days of the Processor's notice. If the Controller objects to any such new criteria, then the Processor may terminate the Agreement upon written notice to the Controller without further liability to the Controller.

3.9 If the Processor wishes to transfer the Personal Data to third parties locating in countries outside of European Economic Area ("EEA"), then the Processor shall ensure the application of the appropriate safeguards by those third parties.

3.10 The Processor shall take all appropriate technical and organizational security measures to prevent the destruction, loss or alteration, unauthorized disclosure of Personal Data or unauthorized access to such data, either accidentally or unlawfully.

3.11 If so requested by the Customer and within the timeframes as reasonably determined by the Customer, the Processor shall supply the Customer with full details of the technical and organizational measures in place to safeguard the security of the Personal Data and compliance with this Appendix 2. The Processor shall enable the Customer to carry out security audits and take all necessary steps to verify the implementation of the technical and organizational security measures. All costs related to the fulfilment of the obligations specified herein, incl. costs related to the organization of an audit shall be borne by the Customer. If the fulfilment of the obligations specified herein bring along any costs or loss of revenue to Processor, the Processor has the right to claim reimbursement of costs or loss of revenue from the Customer.

3.12 The Processors shall notify the Customer without undue delay if it becomes aware of any Personal Data Breach. The information notified to Customer shall describe the nature of the Personal Data Breach, incl., where possible the following:

3.12.1 the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
3.12.2 the name and contact details of the data protection officer or other contact point where more information can be obtained;
3.12.3 the description of the likely consequences of the Personal Data Breach; and
3.12.4 the description of the measures taken or proposed to be taken to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4 LIABILITY

4.1 The liability of the Processor under this Agreement will be limited to the maximum extent permitted by law. The Processor is not liable for the loss of profit, indirect loss and non-patrimonial damage, incl. any indirect or consequential damages. The total liability of the Processor for any kind of damages under this Agreement is in any case limited to EUR 1,000.

4.2 The Processor shall not be liable for any damages arising from the Customer's willful misconduct in Processing the Personal Data.

5 TERM AND TERMINATION

5.1 This Agreement becomes effective when signed by both Parties and remains in force until the fulfilment of the obligations arising from the provision of Service or the Service Agreement.

5.2 Either Party has the right to terminate the Agreement by written notice to the other Party by giving 30

days' advance notice. For the sake of clarity, provision of Service or the Service Agreement shall not be possible without valid Agreement in force.

5.3 The parties agree that upon the termination of the Agreement, the Processor shall return all the Personal Data transferred and the copies thereof to the Customer or shall destroy all the Personal Data and certify in writing to the Customer that it has done so, unless legislation imposed upon the Processor prevents it from returning or destroying all or part of the Personal Data transferred. In that case the Processor is obligated to ensure the confidentiality of Personal Data transferred by the Customer and cease for further Processing of the Personal Data.

6 MISCELLANEOUS

6.1 This Agreement, along with any appendices attached hereto and incorporated herein by reference, sets forth the entire agreement between the Parties in this subject matter and supersedes any prior proposals and representations between the Parties, whether written or oral.

6.2 Unless otherwise stipulated in Service Agreement or this Agreement, any amendments and supplements to this Agreement shall be submitted to Customer no later than thirty (30) days before their proposed date of entry into force. Customer may either approve or indicate disapproval of the amendments before their proposed date of entry into force. The amendments shall be deemed to have been approved, unless the Customer indicates disapproval before their proposed date of entry into force. If Customer disapproves amendments, it may terminate this Agreement free of charge and with immediate effect. The Processor shall be entitled not to notify the Customer about editorial changes.

6.3 This Agreement is governed by and construed in accordance with the laws of Estonia. Any dispute, controversy or claim arising out of or relating to this Agreement, or the breach, termination or validity thereof will be finally settled by Harju County Court as the court of first instance.

APPENDIX 1. DETAILS ON PERSONAL DATA PROCESSING

1. Categories of Personal Data and Data Subjects

1.1. The Personal Data concern the following categories of individuals and Personal Data:

- Customer's customers: name, billing address, contact email, contact phone, VAT number, agreements with the Customer, evidence of actual location for EU VAT purposes, billing and payment data related to the business transactions with the Customer.
- Customer's suppliers: name, contact address, contact email, VAT number, agreements with the Customer, payment data related to the business transactions with the Customer.
- Customer's management board member and shareholder: name, personal identification code, date of birth, contact postal address, contact email, nationality, gender, video recording, including facial image, other relevant personal details.
- Customer's employees: name, personal identification code, contact postal address, contact email, contact phone, agreements with the Customer, type of employment, start date of employment, job title, location of employment, end date of employment and the basis of termination, person's status in Estonian Employment Register, salary data, business trips and the related documents, purchases by the person on behalf of the company, business-related payments to the person from the Customer's account.
- Individuals authorized by the Customer to use Processor's Services on behalf of the Customer: name, gender, personal identification code, date of birth, nationality, contact postal address, contact email, start date and end date of the authorization.
- Customer's transaction data on bank account in Processor's partner bank or other credit or payment institution, to which the Customer has granted access to Processor for the purpose of provision of Service: initiators and recipients of the payments, payment details, payment essence and description of transactions, transactions overviews, account statements, usage of payment cards, payment card transactions etc.
- Customer's use of Service: use of the website, platform, interfaces by representatives, who are natural persons and their communication and information submitted by them to the customer support.
- Customer's and persons' related to Customer investigations, checks, claims: AML checks, fraud cases, chargebacks, reimbursement of claims, debts, fines, negative balances.

2. Purposes of the data Processing

2.1. The Personal Data will be processed by the Processor for the following purposes during the provision of Service:

- Registration and administration of the Customer in Estonian Commercial Register
- Address and/or contact person service
- Customer's billing and payment collection
- Customer's accounting in Estonia
- Customer's tax reporting and payment in Estonia
- Customer's compliance in Estonia
- Customer's access to Processor's partner bank and Customer's utilizing of the banking services provided by the partner bank, including provision by the Processor of technical and supportive services related to the banking services (web interface, gathering of documentation, integration of electronic identification, customer support etc.)
- Customer's access to any other services as Processor and Customer may additionally agree

3. Processing activities

3.1. The Personal Data will be subject to the following Processing activities and processing by the following IT solutions of the Processor and third-party processors:

- Creation, submission, collection, storage, structuring, processing (including digitalization), modification, deletion of Customer's sales and cost documents and data, and related agreements - Processor's software solution (Estonia), Flex Fulfilment (EU), Eesti Post (Estonia), Avalara INC, WebinGO OÜ (Estonia), E-Residency HUB (Estonia)

- Preparation of payments, collection, storage, structuring, processing, modification, deletion of Customer's payment transaction data - Processor's software solution, SmartAccounts.
- Matching of payment transaction data and sales/cost documents and data: Processor's software solution, SmartAccounts.
- Collection, storage, structuring, processing, modification, deletion of Customer's business trip data and documents - Processor's software solution, SmartAccounts.
- Collection, storage, structuring, processing, modification, deletion of Customer's employment agreements and salary data - Processor's software solution, SmartAccounts.
- Making the data and documents listed above available to the Customer's authorized representatives via the Processor's software solution.
- Analysis of Customer's business activities and transactions from the accounting and compliance perspective - Processor's software solution, SmartAccounts.
- Registration of the Customer in Estonian Commercial Register, submission of petitions for an entry regarding alteration or dissolution in Estonian Commercial Register: Processor's software solution, Estonian Company Registration Portal.
- Registration and reporting of employment data and documents to Estonian Tax authorities: Processor's software solution, Estonian e-Tax services.
- Submission of Customer's tax reports to Estonian Tax authorities: Processor's software solution, Estonian e-Tax services.
- Hosting, data and file storage, backup of Processor's software solution: Amazon Web Services (Ireland).
- Provision of a Customer-facing interface, which will connect to the Processor's partner bank backend giving access to the Customer account in the partner bank, incl. enabling the Customer to apply for the personal account, conclude an agreement with the Processor's partner bank, activate or unlock the card, change the Customer's personal data, initiate payments – Processor's Web UI.
- Getting and storing of transactions overviews and account statements on the Customer account opened in the Processor's partner bank and balance and transactions overviews on payment cards issued by Processor's partner bank - Processor's Web UI.
- Conducting of Customer authorized representative's authentication and authorization – ID card, Smart ID.
- Provision of access to the payment accounts of the Customers opened in the Processor's partner bank by using third party service providers (i.e. payment initiation and account information service providers - TPPs) – Processor's software solution.
- Conducting of Customers' and Customers' authorized representatives' KYC and KYB checks - Processor's software solution, integrations with third party service providers (e.g. IDnow).
- Provision of customer support, including customer support related to the banking services provided by the Processor's partner bank – Processor's and Processor's partner bank's physical and electronical, including by telephone customer support.
- Marketing and distribution of Service – Processor's and its cooperation partners', including Processor's partner bank, services.
- Sales data collection, and file storage.
- International VAT TAX return provider for TAX return, Intrastat data

APPENDIX 2. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES APPLIED BY THE PROCESSOR

1. Applicable measures

1.1. Processor is using industry-standard Transport Layer Security (TLS) encryption technology to safeguard all sensitive/credit information supplied by the Customer, and Processor also employs application-layer security features to further anonymize Personal Data.

1.2. Processor assigns the access rights to the Personal Data Processing system to the minimum extent necessary for the provision of Service. The Processor confirms that access to any Personal Data is provided only to its employees who need the access for the provision of Service.

1.3. Processor cancels the access right of the Personal Data Processing system without delay when the Personal Data handler is changed due to the personnel shift or retirement.

1.4. When a Processor issues a user account that can access the Personal Data Processing system, it is issuing a user account for each Personal Data handler and shall not share it with other Personal Data handler.

1.5. Personal Data is accessible through a secure electronic personal identification with an ID-card.

1.6. Processors servers are located within enterprise-grade hosting facilities that employ robust physical security controls to prevent physical access to the servers they house. These controls include 24/7/365 monitoring and surveillance, on-site security staff and regular ongoing security audits.

1.7. Processor is using multi location data backup servers which are configured to perform full, incremental, and differential data backup and follow a predefined schedule.

1.8. Services provided by the Processor works on 256 bit TLS encryption which ensures that Personal Data is transmitted in a secure and safe environment. It also prevents data snooping during transmission.

2. Prevention from malicious programs

2.1. Processor has installed firewall protections to all its servers that can prevent and treat malicious programs, and maintain the latest status through automatic update of the security program.

2.2. Processor's security team is continuously monitoring event logs, notifications and alerts from all systems to identify and manage threats.

3. Information security incident management

3.1. Information security events are reported to the Customer as quickly as possible.

3.2. All employees of the Processor are aware of the procedure for reporting information security events and the point of contact to which the events should be reported.