DATA PROCESSING AGREEMENT

This Data Processing Agreement (DPA) is part of the General Payment Processing Service Terms and Conditions for Merchants (hereafter “Agreement”).

1. Parties

The Parties of this DPA are the Parties mentioned in the Agreement.

The Data Controller is the Merchant who has signed the Agreement.

Data Processor:

Paytrail Plc
Business ID: 2122839-7
Lutakonaukio 7
40100 Jyväskylä
Finland

2. Background

The processor of Personal Data shall provide services to the Data Controller in accordance with the Agreement. In conjunction with providing services, the processor of Personal Data shall process the Personal Data of the Data Controller’s customers, employees or other persons.

This Data Processing Agreement is intended to ensure the Personal Data protection and information security when the processor of Personal Data handles Personal Data on behalf of the Data Controller.

3. Definitions

‘Personal Data’ means any information relating to an identified or identifiable natural person. An identifiable natural person is a person who can be identified directly or indirectly using identifiers such as name, address, personal identification number, subscription number, IP address, location data, domain, transmission of data or message content, or based on one or more their physical, physiological, genetic, psychological, economic, cultural or social characteristics.

Otherwise, the definitions stated in the Agreement shall be followed.

4. Data Controller's Obligations

In relation to the Agreement between the Parties, the Data Controller acknowledges and confirms that the processing of Personal Data is compliant with the applicable data protection legislation. In particular, the Data Controller ensures:

1) The processing of Personal Data is based on legitimate purposes within legal limits.
2) The registered individuals have been duly informed about the processing of Personal Data.
3) The Data Controller has the right to transfer Personal Data to the processor of Personal Data for processing.

The Data Controller shall instruct the Data Processor on the processing of data as follows:

The Data Controller ascertains that this Data Processing Agreement and the lawful instructions given by the Data Controller provide reasonable guarantees that the data processing performed by the processor of Personal Data pursuant to the Agreement meets the requirements of the applicable data protection legislation. Any modifications to the data processing instructions shall be mutually agreed upon by the Parties.

DATA PROCESSING INSTRUCTIONS

Data should be handled with the utmost care and the following instructions shall be used in order to ensure the proper processing of Personal Data.

- Information provided by the Data Controller shall only be processed to provide or maintain the payment service based on a justified need.
- A digital trace must always be left in the processing history when viewing Personal Data in the Data Processor's system.
- Any documents disclosed by the Data Controller that relate to Personal Data shall be destroyed without delay and in secure manner after use.
- The Data Processor is obligated to keep Personal Data undisclosed and confidential.

5. Data Processor's Obligations

The processor of Personal Data may only handle Personal Data in accordance with the documented instructions defined in the Data Processing Agreement.

The Data Processor uses the following subcontractors:

Vakka-Suomen Puhelin Oy
Business ID: 0213072-2
Pohjoistullikatu 11
23500 UUSIKAUPUNKI
Finland

Finnchat Oy
Business ID: 2472559-1
Ylistönmäentie 24
40500 JYVÄSKYLÄ
Suomi

The subcontractors shall observe the same data processing principles and obligations as the undersigned Data Processor. The subcontractors shall be given written instructions on handling Personal Data.

Before changing or adding subcontractors involved in processing Personal Data, the Data Processor shall notify the Data Controller in writing without undue delay. If the Data Controller does not accept the change or addition of a subcontractor, the Data Controller shall be entitled to terminate the Agreement with a 30 day notice.

As a payment institution, the Data Processor is required to retain payment information for a duration of five years as outlined in the Act on Detecting and Preventing Money Laundering and Terrorist Financing. After the five year period, the payment information shall either be deleted or anonymized.

6. Data Disclosure Outside the EU

Personal Data may be transferred outside the European Union or European Economic Area in accordance with data protection legislation. The Data Controller shall, at any time, have the right to obtain information from the Data Processor on the location of the processing of Personal Data.

7. Data Security

The Data Processor acknowledges the potential risks associated with the service provided and takes into account any administrative and technical measures needed to minimize the risk of unauthorized use of Personal Data provided by Data Controller and processed by Data Processor. In addition, the Data Processor shall take any necessary measures to ensure the integrity and availability of the information.

The Data Processor ensures that personnel handling Personal Data have received relevant training and instruction for processing Personal Data.

The Data Processor shall include, but not be limited to, the following security measures to protect the Personal Data:

- Personal Data encryption
- Minimization of access control and access rights
- Technical solutions to encrypt data transfers
- Administrative data security
- Risk management

- Personnel security clearance
- Data security testing of systems

The Data Controller is entitled, as required by data protection legislation, to receive necessary information in order to be able to audit whether the Data Processor complies with its obligations under this Agreement. Each Party shall bear their own audit costs.

8. Security Breach Measures

Upon learning of a Personal Data security breach, the Data Processor shall notify the Data Controller in writing, without undue delay, and within 36 hours of the breach.

The Data Processor shall provide the Data Controller with at least the following information about the security breach:

1) description of the Personal Data security breach;
2) provide contact information of the data protection officer or other responsible person for further information;
3) description of the possible consequences of the Personal Data security breach; and
4) description of the measures the processor of Personal Data proposes or has al ready taken towards the Personal Data security breach and, as appropriate, mea sures to mitigate potential adverse effects.

9. Liability

Each Party shall be responsible for the costs, expenses, indemnities, losses and damages incurred by the other Party as result of action that is contrary to this Data Processing Agreement and/or applicable data protection legislation or a decision made by a competent data processing authority.

10. Agreement Transfer

The transfer of the Data Processing Agreement shall be in accordance with the Agreement.

11. Applicable Law and Disputes

This Data Processing Agreement is subject to the law agreed upon in the Agreement. Any disputes, litigations and claims arising from this Data Processing Agreement shall be settled as agreed upon in the Agreement.