Annex 1

PERSONAL DATA PROCESSING AGREEMENT

This personal data processing agreement (the "**Data Processing Agreement"**) is an annex to the Terms of Service or other agreement (the "**Agreement"**) entered between Botguard OÜ as the service provider (the "**Provider**") and the customer (the "**Customer**") who uses service in accordance with the terms of the Agreement (the Provider and the Customer each also a "**Party"** and collectively the "**Parties"**) under which the Provider provides to the Customer Bot Traffic Management Services (the "**Services**").

In connection with the provision of the Services under the Agreement, the Provider processes certain personal data for the Customer. To ensure the secure, correct and lawful processing of personal data, the Parties have agreed to supplement the Agreement and enter into this Data Processing Agreement as an Annex to the Agreement.

In case of a conflict between the Agreement and the Data Processing Agreement with regard to the processing of personal data, the Data Processing Agreement shall prevail and apply.

1. GENERAL PROVISIONS

1.1. The terms used in the Data Processing Agreement are used in the meaning given to them in Article 4 of the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter the "**GDPR"**) or in the meaning given to them in the Agreement.

1.2. In the context of Article 28 of the GDPR, the Customer is the data controller of the personal data made available to the Provider in the course of the provision of the Services and the Provider is the data processor.

2. GENERAL OBLIGATIONS OF THE PROVIDER

2.1. The Provider shall process personal data only in accordance with the applicable law, the terms of the Agreement and the terms of this Data Processing Agreement.

2.2. The Provider shall process personal data only for the purposes described in Annex A (see below).

2.3. The Provider shall keep records of all the data processing operations carried out on behalf of the Customer in accordance with the requirements under the GDPR.

3. GENERAL OBLIGATIONS OF THE CUSTOMER

3.1. The Customer confirms and warrants that upon using the Services and making available any personal data to the Provider, the Customer has acquired all necessary authorisations and permits as required for that by applicable law and the GDPR.

4. CONFIDENTIALITY

4.1. The Provider shall ensure the confidentiality of the personal data processed on behalf of the Customer.

4.2. The Provider shall ensure that no unauthorised third parties can access the personal data processed on behalf of the Customer, for example, employees of the Provider, who do not need access in relation to the performance of their duties or other service providers of the Provider, who in this specific case do not need access to the personal data in relation to the performance of their duties.

4.3. The Provider shall ensure that all the representatives and employees of the Provider and other persons who through the Provider come into contact with the personal data processed on behalf of the Customer are subject to the confidentiality obligation assumed under a contract or the law and the Provider shall ensure that their representatives, employees and other persons acting for their benefit maintain the full confidentiality of the personal data.

5. SECURITY MEASURES

5.1. The Provider shall ensure the security of personal data processing for the purposes of protecting personal data from accidental or unauthorised processing, disclosure or destruction.

5.2. Taking into account the state of the art and costs of implementation, and the nature, scope, context and purposes of the personal data processing as well as the risk to the rights and freedoms of natural persons, of varying likelihood and severity, that may result from personal data processing, the Provider shall apply appropriate technical and organisational measures upon personal data processing to ensure the security of personal data.

5.3. Upon the application of appropriate technical and organisational measures, the Provider shall ensure the capacity of the applied processing measures to ensure the ongoing confidentiality, integrity, availability and resilience of personal data.

5.4. The Provider shall *inter alia* ensure that upon personal data processing, the Provider shall use up-to-date information technology solutions, the security of which is regularly tested, ensure that access to the Provider's IT systems and premises is regulated and controlled, and ensure the use of up-to-date antivirus and spyware programmes.

5.5. The Provider shall log all data processing operations carried out on behalf of the Customer so that there are log entries on viewing, amending, transferring and deleting personal data.

5.6. The Customer has the right to authorise an auditor to audit the activity of the Provider with regard to the performance of the Data Processing Agreement in accordance with the GDPR. The Customer shall notify Provider of the audit at least 60 days in advance. The Customer or an auditor appointed by the Customer shall carry out the audit during regular working hours and so that the audit interferes with the regular business activity of Provider as little as possible.

6. PERSONAL DATA BREACH

6.1. In case of a personal data breach or suspected personal data breach, the Provider shall as immediately as possible notify the Customer of this. In case of a personal data breach or suspected breach or an incident that is likely to escalate into a personal data breach, the Provider shall send to the Customer a notification about the personal data breach, which shall include at least the following information:

6.1.1. A description of the nature of the personal data breach;

6.1.2. The categories and approximate number of data subjects concerned;

6.1.3. The categories and approximate number of personal data records concerned;

6.1.4. The name and contact details of the data protection officer or other contact person of Provider if applicable;

6.1.5. The likely consequences of the personal data breach, incl. the likely consequences to data subject;

6.1.6. Measures taken or proposed to be taken by Provider to address the personal data breach or measures to mitigate its possible adverse effects.

6.2. The Provider shall send the notification specified in section 6.1 above to the Customer immediately and if possible not later than within 48 hours as of the occurrence of the personal data breach.

6.3. In case and insofar as the Provider is not able to submit the information described in section 6.1 to the Customer within the term set forth in section 6.2, the Provider may submit the information to the Customer in phases but without undue further delay.

6.4. The Provider shall cooperate fully with the Customer for the purposes of preventing personal data breaches. If a personal data breach occurs, Provider shall cooperate fully with the Customer to address the personal data breach as efficiently and quickly as possible and/or mitigate its possible adverse effects.

6.5. The Provider shall document all personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken.

7. SUBPROCESSORS AND TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

7.1. If the Provider uses subprocessors, the Provider shall assume full liability for the subprocessor to process personal data in accordance with the applicable law and this Data Processing Agreement.

8. LIABILITY

8.1. The Provider shall not be liable for any breach of this Data Processing Agreement or applicable law by the Customer.

9. VALIDITY

9.1. The Data Processing Agreement shall be valid as of the moment of conclusion of the Agreement between the Parties until the Provider is processing personal data on behalf of the Customer or until the end of the term of Agreement, whichever is the later.

10. FINAL PROVISIONS

10.1. The Data Processing Agreement is governed by the laws of the Republic of Estonia.

10.2. Disputes arising from the Data Processing Agreement will be resolved by negotiations or in Estonian courts, Harju County Court being the court of first instance.

ANNEX A to the Data Processing Agreement

1. PURPOSE OF DATA PROCESSING

The Provision of the Services to the Customer in accordance with the Agreement.

2. DATA SUBJECTS

Any natural person entering the webpage using the Services

3. CATEGORIES OF DATA

3.1. IP-address used to enter to the webpage, country of location, internet service provider of the person entering the Customer's webpage;

3.2. full HTTP(S)-request of the software and the operating system used by the person entering the Customer's webpage;

3.3. metadata about the connection (TLS handshake data, various properties of network packets) of the person entering the Customer's webpage).

4. PROCESSING OPERATIONS

The Provider processes the data in order to provide the Services in accordance with the terms of the Agreement. Specifically, as a result of data processing the Provider shall determine whether the person accessing the webpage of the Customer is human user, legitimate search engine bot, a malicious bot or hacker and access to the webpage by malicious bot or hacker will be denied.

5. RETENTION

Data collected about each person accessing the webpage shall be retained maximum 3 months.