Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The Customer, as defined in the CleanTalk License Agreement of Service (the “data exporter”)

And

CleanTalk Inc. Address: 711 S Carson street, suite 4, Carson city, NV, 89701 (the “data importer”)

each a ‘party’: together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

‘the data exporter’ means the controller who transfers the personal data;

‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

‘the subprocessor’ means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data
protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:
(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) 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;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11:
(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor’s obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.
On behalf of the data exporter:
Name (written out in full): ...
Position: ...
Address: ...
Other information necessary in order for the contract to be binding (if any):

Signature

On behalf of the data importer:
Name (written out in full): Denis Shagimuratov
Position: Chief Executive Officer
Address: 711 S Carson street, suite 4, Carson city, NV, 89701
Other information necessary in order for the contract to be binding (if any):

Signature

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Data exporter

The data exporter is the legal entity specified as "the User" in the License Agreement.

Data importer

The data importer is CleanTalk Inc. CleanTalk is the provider of the Services to the User as described in the License Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects: Data subjects include the individuals about whom data is provided to CleanTalk via the Services (as defined in the License Agreement).

Categories of data

The personal data transferred concern the following categories of data: Data relating to individuals provided to CleanTalk via the Services by (or at the direction of) Data Exporter.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: Data relating to individuals provided to CleanTalk via the Services by (or at the direction of) Data Exporter.
Purposes of Processing

CleanTalk Inc. shall process personal data as necessary to provide the Subscription Services to data exporter in accordance with the License Agreement.

Duration of Processing

Data processing will be for the period specified in the License Agreement (during the subscription period). Such period will automatically terminate upon the deletion by the Data Importer of all data (the User account).

Data Deletion. During the term of the License Agreement, the Data Importer will provide the Data Exporter with the ability to delete the Data Exporter’s personal data from the Services in accordance with the License Agreement or until Data Exporter deletes the User account information.

Access to Data. During the term of the Services Agreement, the Data Importer will provide the Data Exporter with access to, and the ability to rectify, restrict processing of and export the Data Exporter’s personal data from the Services in accordance with the License Agreement.

Subprocessors. The Data Importer may engage Subprocessors to provide parts of the Services. The Data Importer will ensure Subprocessors only access and use the Data Exporter’s personal data to provide the Services and not for any other purpose.

Processing operations

Personal Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing Activities:

a. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to you; and/or
b. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached): The Data Importer currently abides by the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the License Agreement.
Security Standards

The data importer has implemented and will maintain appropriate technical and organisational measures, internal controls and information security routines intended to protect Customer Data. The technical and organisational measures, internal controls and the information security standards.

Information Security Program. CleanTalk maintains and will continue to maintain an information security program that includes policies, procedures, and controls governing the Processing of Customer Data through CleanTalk. The Information Security Program is designed to protect the confidentiality, integrity, and availability of Customer Data by using a multi-tiered technical, procedural, and people-related control approach in accordance with industry best practices and applicable laws and regulations.

Permitted Use of Customer Data. CleanTalk will not Process Customer Data in any manner other than as permitted or required by the Agreement.

Acknowledgement of Shared Responsibilities. The security of data and information that is accessed, stored, shared, or otherwise Processed via a multi-tenant cloud service such as CleanTalk Cloud Services are shared responsibilities between a cloud service provider and its customers. As such, the Parties acknowledge that: (a) CleanTalk is responsible for the implementation and operation of the Information Security Program and the protection measures described in the Agreement and this Security Attachment; and (b) Customer is responsible for properly implementing access and use controls and configuring certain features and functionalities of Cleantalk Cloud Services that Customer may elect to use Cleantalk Cloud Services in the manner that Customer deems adequate to maintain appropriate security, protection, deletion, and backup of Customer Data.

The Data Importer will implement security requirements for staff and all subcontractors, vendors or agents who have access to Personal Data that are designed to:

Prevent unauthorized persons from gaining access to Personal Data processing systems;

Prevent Personal Data processing systems from being used without authorization;

Ensure that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization;

Ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified;

Ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in or removed from Personal Data Processing;
Ensure that Personal Data are Processed solely in accordance with the Instructions of the Data Controller;

Ensure that Personal Data are protected against accidental destruction or loss; and

Ensure that Personal Data collected for different purposes can be processed separately.

Data Importer will conduct periodic risk assessments and review and, as appropriate, revise its information security practices at least annually or whenever there is a material change in Data Importer’s business practices that may reasonably affect the security, confidentiality or integrity of Personal Data, provided that Data Importer will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability or integrity of Personal Data.

Physical Security. The Data Importer will maintain commercially reasonable security systems at all Data Importer sites at which an information system that uses or houses Personal Data is located. The Data Importer reasonably restricts access to such Personal Data appropriately.

Organizational Security. When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Personal Data stored on them.

Data Importer will implement security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

All Security Incidents are managed in accordance with appropriate incident response procedures.

Network Security. The Data Importer maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.

Access Control. Data Importer will maintain appropriate access controls, including, but not limited to, restricting access to Personal Data to the minimum number of Data Importer personnel who require such access.

Only authorized staff can grant, modify or revoke access to an information system that uses or houses Personal Data.

User administration procedures define user roles and their privileges, and how access is granted, changed and terminated; address appropriate segregation of duties and define the logging/monitoring requirements and mechanisms.

All employees of the Data Importer are assigned unique User-IDs.

Access rights are implemented adhering to the “least privilege” approach.
Data Importer implements commercially reasonable physical and electronic security to create and protect passwords.

Data Importer will encrypt, using industry-standard encryption tools, all sensitive data that Data Importer: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; and (iii) stores on portable devices, where technically feasible. Data Importer will safeguard the security and confidentiality of all encryption keys associated with encrypted Sensitive Information / Personal Data.

Virus and Malware Controls. The Data Importer installs and maintains anti-virus and malware protection software on the system to protect Personal Data from anticipated threats or hazards and protect against unauthorized access to or use of Personal Data.

Data Importer will require personnel to comply with its Information Security Program prior to providing personnel with access to Personal Data. The Data Importer implements a security awareness program to train personnel about their security obligations. This program includes training about data classification obligations; physical security controls; security practices and security incident reporting.

Business Continuity. The Data Importer implements appropriate disaster recovery and business continuity plans. Data Importer regularly reviews and updates its business continuity plan to ensure it is current and effective.

Primary Security Manager. Data Importer will notify Data Exporter of its designated primary security manager upon request. The security manager will be responsible for managing and coordinating the performance of Data Importer's obligations set forth in its Information Security Program and in this Contract.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses')

Clause 4(h) and 8: Disclosure of these Clauses

Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clauses 5(a) and 5(b): Suspension of data transfers and termination

If the data importer has not or cannot cure the non-compliance then the data exporter may suspend and/or terminate the affected part of the Services in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination). The data exporter shall not be required
to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(j): Disclosure of subprocessor agreements

a. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

b. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

c. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably requires in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

a. the data exporter promptly notifying the data importer of a claim;
b. the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.