Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

Data Transfer Agreement

Parties

This Agreement is made between:

(1) **Censornet Limited** (company number 05518629) of Matrix House, Basing View, Basingstoke, RG21 4DZ, England

(hereinafter the "**data exporter**");

and

(2) **Apriorit LLC** (D-U-N-S number: 117063762) 8 The Green, Suite #7106, Dover, DE 19901
United States (hereinafter 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:

a) "**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;

b) "**the data exporter**" means the controller who transfers the personal data;

c) "**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;

d) "**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;

e) "**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;

f) "**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

a) 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(a) and (b), Clause 7, Clause 8(b), and Clauses 9 to 12 as third-party beneficiary.

b) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), 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.

c) The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), 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.

d) 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(c) 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

a) 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.

b) 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 of by operation of law, in which case the data subject can enforce its rights against such entity.

c) The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

d) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs (a) and (b), 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.

e) 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:
   i) the data exporter promptly notifying the data importer of a claim; and
   ii) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

Clause 7

Mediation and jurisdiction

a) 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:
   (i) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (ii) to refer the dispute to the courts in the Member State in which the data exporter is established.

b) 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

a) 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.

b) 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.

c) 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 (b). 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

a) 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.

b) Additional commercial clauses have been added as follow:
   (i) Clause 6(e) (Liability); and
   (ii) Clause 13 (Counterparts).

Clause 11

Subprocessing

a) 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.

b) 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 (a) 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.

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

d) 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

a) 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.

b) 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 (a).

Clause 13

Counterparts

This contract may be entered into by the parties in any number of counterparts. Each counterpart shall, when executed and delivered, be regarded as an original, and all the counterparts shall together constitute one and the same instrument. This contract shall take effect for any data exporter or data importer when such party has executed the contract.

On behalf of the data exporter:

Name: Laura Harding

Position: Commercial Operations Manager

Address: Censornet Limited, Matrix House, Basing View, Basingstoke, RG21 4DZ

Other information necessary in order for the contract to be binding (if any): N/A

Signature:

On behalf of the data importer:

Name: Dennis Turpitka

Position: CEO

Address: 8 The Green, Suite #7106, Dover, DE 19901 United States

Other information necessary in order for the contract to be binding (if any): N/A

Signature: ________________________________

APPENDIX 1

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the Transfer

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

- a provider of Cloud Security Services, including email security

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

- a software developer, who may have access to Censornet's customers / end users' Personal Data in the form of sent and received email messages, in performing its Services.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- Censornet's Customers, Clients and Prospects (including its staff)

Categories of data

The personal data transferred concern the following categories of data (please specify):

- Basic personal data (for example street name and building number or name (address), postal code, city, country, mobile phone number, first name, last name, initials, email address, domain and related data);
- Authentication data (for example user name, password, audit trail);
- Contact information (for example addresses, email, phone numbers, website address);
- Device identification / Unique identification numbers (for example IP addresses, MAC addresses, logical tag);
- Commercial Information (subscription (license) information, purchase history, payment history);
- Location data (for example, geo-location network data);
- Email activity (inbound and outbound email messages, including attachments);
- Internet activity (for example browsing activity, cloud application activity);
- Any other personal data identified in Article 4 of the GDPR.

Summary of Data Processed (input / output data)

Email Security (EMS)	• Inbound and outbound email messages (including attachments) sent or received externally to or from the organization	• Log data relating to inbound and outbound email messages sent or received externally. Log information includes IP addresses, To, From and Subject fields, server responses, and other metadata, but does not include the message body or any file attachments

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

None

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

Customers' issues bugfix
Apriorit has the access to the customers' emails, dump files, log files and esmaster/esdata databases which contain personal data. For bugfix purposes emails, dumps and logs can be parsed, customers' emails can be processed on the testing environment.

Deployment/rollback
Apriorit has the access to all servers, which are being updated during deployment or rollback. Apriorit has the access to the servers with the 3rd party services (for example the GeoIP, Vade). It is possible to see personal data such as email address, name, IP address in the 3rd party libraries logs. Apriorit can update databases, including customers rules.

New features implementation
During the implementation of the new features, Apriorit can use the data from esmaster/esdata databases, mostly it's the information about customers' rules.

DATA EXPORTER

[ ]

Name: Laura Harding

Authorised Signature

DATA IMPORTER

[ ]

Name: Dennis Turpitka

Authorised Signature

APPENDIX 2

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer shall undertake appropriate technical and organisational measures to protect against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The measures taken should take into account available technology and the cost of implementing the specific measures and must ensure a level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

1. Access control of processing areas

Data Importer implements suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment used to process the personal data. This is accomplished by:
- Card key systems
- Building receptionists

2. Access control to data processing systems

Data Importer implements suitable measures to prevent its data processing systems from being used by unauthorised persons. This is accomplished by:
- Unique user ID and privacy password for each employee
- Mandatory password change on a regular basis
- Lock out of user accounts after a pre-determined number of failed log-in attempts
- Anti-virus and spam scanning

3. Access control to use specific areas of data processing systems

Data Importer ensures that the persons entitled to use its data processing systems are only able to access the data within scope and to the extent covered by their respective access permission (authorisation) and that the personal data cannot be read, copied or modified or removed without authorisation. This shall be accomplished by:
- User IDs set up to restrict user privileges based on job duties, project responsibilities and other business activities
- VPN access requires authorisation and authentication

4. Transmission control

Data Importer implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged. This is accomplished by:
- Firewall and encryption technologies to protect gateways and pipelines through which the data travels
- Monitoring of encryption technologies

5. Access and input control

Data Importer implements suitable measures to ensure that it is possible to check and establish whether, when, by whom and for what reason personal data have been input into data processing systems or otherwise processed. This is accomplished by:
- Authentication of the authorised personnel via utilisation of user ID and passwords
- Restricted physical access to processing areas
- System time-out after non-activity for a pre-determined time period

6. Instructional control

Data Importer ensures that personal data may only be processed in accordance with the Agreement and Data Exporter's instructions. This is accomplished by:

- Information & security training and policies & procedures for employees

7. Availability control

Data Importer implements suitable measures to ensure that personal data are protected from accidental destruction or loss. This is accomplished by:

- Business continuity, backup and disaster recovery management
- Offsite backup storage

8. Separation of processing for different purposes

Data Importer implements suitable measures to ensure that personal data that are intended for different purposes can be processed separately. This is accomplished by:

- Access to personal data being restricted via user authorisation passwords
- Use of personal data being application specific

DATA EXPORTER

Name: Laura Harding

Authorised Signature:

DATA IMPORTER

Name: Dennis Turpitka

Authorised Signature ______________