DATA PROCESSING EXHIBIT (the "DPE")

The DPE forms part of the Cloudamize License Agreement between Cloudamize, Inc. and You (the "**Agreement**") under which Cloudamize provides the Services to You. Terms not defined in this DPE shall have the meaning given to them in the Agreement. If any term in this DPE conflicts with any term in the Agreement then this DPE shall prevail.

This DPE shall apply only if the Services require the transfer of Personal Data (as defined below) to a country outside of the European Economic Area or to a country without an adequate level of protection, as determined by the European Commission.

AGREED TERMS

1. DEFINITIONS

"**Your Data**" means any and all data, content or information entered into, transmitted through, or stored on the Services by You or Your Users, or otherwise made available or accessible to Cloudamize by You or Your Users.

"Data Protection Laws" means all data protection laws applicable to the Processing of Personal Data under this DPE, including local, state, national and/or foreign laws, treaties, and/or regulations, EU Data Protection Laws, and implementations of EU Data Protection Laws into national law.

"EU Data Protection Laws" means: (i) up to 25 May 2018, the Data Protection Directive 95/46/EC; and (ii) from 25 May 2018 onwards, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**").

"Personal Data" means any Customer Data that relates to an identified or identifiable natural person ("**Data Subject**").

"**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.

"Processing or Process" means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

"Standard Contractual Clauses" means the Standard Contractual Clauses for the transfer of personal data to processors established in third countries pursuant to Commission Decision (2010/87/EU), as set out in Appendix B to this DPE.

"**Subprocessor**" means a Cloudamize Affiliate or third-party entity engaged by or on behalf of Cloudamize or a Cloudamize Affiliate to process Personal Data.

"**Valid Transfer Mechanism**" means a data transfer mechanism permitted by EU Data Protection Laws as a lawful basis for transferring Personal Data to a recipient outside the EEA.

"**Special Categories of Personal Data**", "**Data Processor**" and "**Data Controller**"; shall have the

meaning given to it in the GDPR.

2. PROCESSING PERSONAL DATA

2.1 Scope and Role of the Parties. This DPE applies to the Processing of Personal Data by Cloudamize in the course of providing the Services. For the purposes of this DPE, You are the Data Controller and Cloudamize is the Data Processor, Processing Personal Data on Your behalf. Cloudamize shall Process Personal Data to provide the Services to You. The duration of the Processing shall be for the term of the Agreement. The types of Personal Data and categories of Data Subjects are set forth in Appendix 1 to the Standard Contractual Clauses, which is hereby incorporated into this DPE by reference.

2.2 Instructions for Processing. Cloudamize shall Process Personal Data in accordance with Your documented instructions unless We are required by law to do otherwise. You hereby instruct Cloudamize to Process Personal Data to provide the Services in accordance with the Agreement (including this DPE) and any Order Form.

2.3 Compliance with Laws. We shall comply with all Data Protection Laws applicable to Us in our role as a Data Processor. For the avoidance of doubt, We are not responsible for complying with Data Protection Laws applicable to You, Your Users, or Your specific industry standards such as those not generally applicable to Our industry. You shall comply with all Data Protection Laws applicable to You as a Data Controller.

2.4 Confidentiality. We shall ensure that all personnel who have access to and/or process Personal Data are obliged to keep Personal Data confidential.

2.5 Lawful transfer of Personal Data. YOu shall ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to Us for the duration and purposes of this DPE.

2.6 Restriction of access. You shall restrict Our access to Personal Data to those types of access that are unavoidable for Cloudamize to provide the Services. In no event shall Cloudamize, its employees, agents and Subprocessor(s) be liable to You to the extent that the processing of personal data is based on Customer's failure to restrict Our access to Personal Data to those types of access that are unavoidable for Us to provide the Services.

2.7 Reliance on Customer. You acknowledge that We are reliant on You for direction as to the extent to which We are entitled to process Personal Data on behalf of You for the provision of the Services. Consequently, Cloudamize will not be liable under this DPE for any claim brought by a data subject arising from any action or omission by Us to the extent that such action or omission resulted directly or indirectly from any of the following: Our processing of Personal Data in accordance with this DPE, Your instructions, or Your failure to comply with its obligations under the applicable Data Protection Laws.

3. SUBPROCESSORS

3.1 Use of Subprocessors. Customer specifically authorises the engagement of Our Affiliates as Subprocessors. In addition, You generally authorize the engagement of any Subprocessors provided that such Subprocessors have entered into a written agreement with Us or Our Affiliate requiring the Subprocessor to abide by terms no less protective than those provided in this DPE. We shall be liable for the acts and omissions of any Subprocessors to the same extent as if the acts or omissions were

performed by Cloudamize.

3.2 Notification of new Subprocessors. We shall make available to You a webpage with a list of Subprocessors authorised to Process Personal Data ("**Subprocessor List**") and provide You with a mechanism to obtain notice of any updates to the Subprocessor List. The Subprocessor List shall be located at: [https://www.cloudamize.com/subprocessors] {or such other URL as We may provide from time to time).

3.3 Clarification to the Standard Contractual Clauses. For the purposes of Clause 11 of the Standard Contractual Clauses, You consent to Us appointing Subprocessors in accordance with clause 3 of this DPE.

4. DATA TRANSFER

4.1 Access to Personal Data and Processing locations. In order to provide the Services to the Customer, We and Our Subprocessors will only access and process Personal Data from (i) countries in the EEA, (ii) countries or territories formally recognised by the European Commission as providing an adequate level of data protection ("**Adequate Countries**") and (iii) third countries or territories provided Cloudamize and the relevant Subprocessor have put a Valid Transfer Mechanism in place.

4.2 Transfer of Personal Data to third countries. Subject to clause 4.1 We shall only transfer Personal Data to, or process Personal Data, outside of the EEA if the following conditions are fulfilled:

(i) We have ensured that a Valid Transfer Mechanism is in place in relation to the transfer;
(ii) the Data Subject has enforceable rights and effective legal remedies;
(iii) We comply with its obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and
(iv) We comply with reasonable instructions notified to it in advance by You with respect to the processing of the Personal Data.

4.3 Standard Contractual Clauses. The parties agree that the Services to be provided to You and Your Affiliates by Us and Our Affiliates may require the transfer of Personal Data outside of the EEA, and that in such event Personal Data will be transferred in reliance on the Standard Contractual Clauses. All transfers of Personal Data out of the EEA and Switzerland shall be governed by the Standard Contractual Clauses which shall apply between You and Your Affiliates (each as "data exporter") and Us (as "data importer").

5. RIGHTS OF DATA SUBJECTS

We shall, in relation to any Personal Data processed in connection with the performance by Us of Our obligations under this DPE:

(a) assist You in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(b) maintain complete and accurate records and information to demonstrate its compliance with this DPE.

6. RETURN AND DELETION OF PERSONAL DATA

We shall at Your written direction, delete or return Personal Data and copies thereof to You on termination of this DPE unless required by Data Protection Laws or other applicable laws to store Personal Data.

7. INFORMATION SECURITY

7.1 Information Security Programme. We shall implement and maintain a written information security programme including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

7.2 Technical and organisation safeguards. We shall implement, and at all times during this DPE maintain technical and organisational safeguards to protect Personal Data from unauthorised or unlawful processing or accidental loss or damage:

(i) ensuring in each case a level of security appropriate to the risk, including in relation to any Special Categories of Personal Data; and

(ii) in addition maintaining controls in line with accepted industry practices including the International Organization for Standardization's standards: Requirements and ISO/IEC 27002 – Code of Practice for International Security Management, the Control Objectives for Information and related Technology (COBIT) standards, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or a SOC type II controls.

7.3 Minimum safeguards. At a minimum, Our safeguards for the protection of Personal Data shall include:

(i) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;

(ii) implementing network, application, database, and platform security;

(iii) securing information transmission, storage, and disposal;

(iv) implementing authentication and access controls within media, applications, operating systems, and equipment;

(v) encrypting Personal Data at rest where possible;

(vi) encrypting Personal Data transmitted over transit in network;

(vii) strictly segregating Your Data from information of Ours or Our other customers so that Your Data is not commingled with any other types of information;

(viii) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Your sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing;

(ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law;

and

(x) providing appropriate privacy and information security training to Your employees.

7.4 Your Security Responsibilities. You shall be solely responsible for:

(i) ensuring a level of security appropriate to the risk in respect of Your Data; and

(ii) backing up Your Data in line with industry best practices.

8. PERSONAL DATA BREACH PROCEDURE

8.1 Your security contact. You shall provide Us with the name and contact information for an employee of Yours who shall serve as Our primary security contact and shall be available to assist Us in resolving obligations associated with a Personal Data Breach.

8.2 Notification of Personal Data Breaches. In the event We become aware of a Personal Data Breach it shall without undue delay notify You by contacting Your security contact using the information provided by You in accordance with clause 8.1. To the extent You require additional information from Us to meet its Personal Data Breach notification obligations under applicable Data Protection Laws, We shall provide reasonable assistance to provide such information to You taking into account the nature of Processing and the information available to Us.

9. OVERSIGHT OF SECURITY COMPLIANCE

Upon Your written request providing reasonable notice to Us and no more than once a year, We grant You or, upon Your election, a third party on Customer's behalf, permission to perform an assessment, audit, examination, or review (the "**Audit**") during business hours of all controls in Our physical and/or technical environment in relation to all Personal Data being handled and/or services being provided to You pursuant to the Agreement. Such an Audit shall be conducted at Your expense and We shall reasonably cooperate by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Data for You pursuant to this DPE. The duration of the Audit shall under no circumstances exceed 2 business days.

Appendix A - 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.

Name, address, and email of the data exporting organization shall be as indicated on the applicable Order Form.

Other information needed to identify the organisation:

For itself and/or on behalf of any Customer Affiliates established in the EEA or Switzerland

(each a '**data exporter'**)

And

Name of the data importing organisation:

Address:

Email: info@cloudamize.com

Other information needed to identify the organisation:

(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

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 of 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.

Appendix 1 to the Standard Contractual Clauses

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

Data importer
The data importer is Cloudamize, a cloud software provider.

Data subjects
The personal data transferred may concern the following categories of data subjects: Your employees, contractors, suppliers, and customers, as the case may be, depending on the Services, and the databases, files shares, and/or data repositories made available to Us.

Categories of data
The personal data transferred may concern the following categories of data: names, email addresses, telephone numbers, cloud provider access credentials, work IP addresses as necessary to provide the Services, and potentially additional Personal Data, depending on the content of Your databases, file shares, and/or data repositories accessible to Us.

Special categories of data (if appropriate)
The personal data transferred is dependent on the content of Your databases, file shares, and/or data repositories made accessible to Us.

Processing operations
The personal data transferred will be to the extent necessary for Us to provide the Services to You, and pursuant to Your instructions.

Appendix 2 to the Standard Contractual Clauses

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 implement and maintain a written information security programme including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

Data importer shall implement and maintain technical and organisational safeguards to protect Personal Data from unauthorised or unlawful processing or accidental loss or damage:

(i) ensuring in each case a level of security appropriate to the risk, including in relation to any Special Categories of Personal Data; and

(ii) maintaining ISO 27001 or similar certification; and

(iii) in addition maintaining controls in line with accepted industry practices including the International Organization for Standardization's standards: Requirements and ISO/IEC 27002 – Code of Practice for International Security Management, the Control Objectives for Information and related Technology (COBIT) standards, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or a SOC type II controls.

At a minimum, data importer's safeguards for the protection of Personal Data shall include:

(i) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;

(ii) implementing network, application, database, and platform security;

(iii) securing information transmission, storage, and disposal;

(iv) implementing authentication and access controls within media, applications, operating systems, and equipment;

(v) encrypting Personal Data at rest where possible;

(vi) encrypting Personal Data transmitted over transit in network;

(vii) strictly segregating data exporter's Personal Data from information of data importer or its other customers so that data exporter's Personal Data is not commingled with any other types of information;

(viii) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at data importer's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing;

(ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and

(x) providing appropriate privacy and information security training to data importer's employees.