Data Privacy Addendum ("DPA")

If you, the Customer, are located in the European Economic Area, and subscribe to any of Arista's Cloud Services memorialized in an agreement between the parties, which may be defined as a cloud subscription agreement or a master services agreement (the "Agreement"), you and Arista agree to the following terms:

1. To the extent that any Agreement contains any terms or conditions that are inconsistent with the following terms, these DPA terms shall supersede. All other provisions of any Agreement shall remain in full force and effect.

2. A new Data Privacy Exhibit, as set forth below, is added to the Agreement and forms an integral part thereof.

DATA PRIVACY EXHIBIT

In delivering the services under the Agreement, Arista and its worldwide corporate entities may process Personal Data provided by or on behalf of Customer. Arista takes the protection and privacy of this data seriously, will ensure that its partners protect this data with at least the same level of care, and will not use the data other than as described herein.

1. DEFINITIONS

1.1 "Applicable Privacy Law(s)" means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, EU Data Protection Law.

1.2 "Authorized Persons" means any person who processes Personal Data on Arista's behalf, including Arista's employees, officers, partners, principals, contractors and Subcontractors.

1.3 "Cloud Services" means the Subscription Services described in the Agreement and to which Customer subscribes.

1.4 "Customer Employee Data" means any Personal Data of an employee, officer, partner, principal, contractor, intern, or other member of Customer.

1.5 "EU Data Protection Law" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR").

1.6 "Personal Data" means information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. For the avoidance of doubt, Personal Data includes personally identifiable information.
1.7 “Security Incident” means any unauthorized or unlawful breach of security leading to the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to Personal Data.

1.8 “Service Personal Data” means any Personal Data that Customer or Customer’s end users process through the Cloud Services.

1.9 “Standard Contract Clauses” or “SCCs” means the clauses set forth in Annex A which have been approved by the European Commission, on or about June 2021, as a legal basis for the transfer of Personal Data to a third country being any country outside the European Economic Area (EEA).

1.10 “Subcontractor” means any third party (including any Arista Entity) engaged to process any Personal Data relating to this DPA and/or the agreements between Arista and Customer; Subcontractor is equivalent to “sub-processor” under the SCCs.

1.11 “Arista Entity” means any entity that Arista Networks, Inc. controls (directly or indirectly), where “control” means at least fifty percent (50%) ownership of the outstanding shares of the entity, or the ability to direct the management of the entity by contract or otherwise.

1.12 The terms “Data Controller” / “Controller”, “Data Processor” / “Processor”, “Data Subject” and “processing” have the meanings given to them in Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given in EU Data Protection Law will apply.

2. ROLE AND SCOPE OF PROCESSING

2.1 Arista and Customer will comply with all applicable requirements of the Applicable Privacy Laws. Arista shall process Service Personal Data through the Cloud Services only as a Processor acting on behalf of Customer (whether as Controller or itself a Processor on behalf of third party Controllers). Customer has ensured and will continue to ensure that it has the rights to transfer both the Service Personal Data and any relevant Customer Employee Data to Arista for the duration and purposes of the Agreement.

2.2 Arista will at all times:
   a. process the Personal Data only for the purpose of (1) providing the Services to Customer under the Agreement; (2) contacting Customer regarding any support for such Services or the pending or potential sale or license of Arista’s products and Services; or (3) improving the Services, each of the foregoing items (1)-(3) in accordance with Customer’s documented instructions including this DPA (except where otherwise required by applicable law);
   b. not process the Personal Data for its own purposes or those of any third party;
   c. if Arista is required by any applicable law to process such Personal Data for other purposes, promptly notify Customer of such other purposes before performing the processing required, unless such law prohibits notifying Customer;
   d. ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of Personal Data and against
accidental loss or destruction of, or damage to, Personal Data, appropriate to the
harm that might result from the unauthorised or unlawful processing or accidental
loss, destruction or damage and the nature of the data to be protected, having
regard to the state of technological development and the cost of implementing any
measures (those measures may include, where appropriate, pseudonymising and
encrypting Personal Data, ensuring confidentiality, integrity, availability and
resilience of its systems and services, ensuring that availability of and access to
Personal Data can be restored in a timely manner after an incident, and regularly
assessing and evaluating the effectiveness of the technical and organisational
measures adopted by it);

e. ensure that all Arista personnel who have access to and/or process Personal Data
are obliged to keep the Personal Data confidential;

f. assist Customer, at Customer's cost, in responding to any request from a Data
Subject and in ensuring Customer's compliance with its obligations under the Data
Protection Legislation with respect to security, breach notifications, impact
assessments and consultations with supervisory authorities or regulators;

g. at the written direction of Customer, delete or return Personal Data and copies
thereof to Customer on termination of the Agreement unless required by
Applicable Laws to store the Personal Data;

h. maintain complete and accurate records and information to demonstrate its
compliance with this DPA and allow for audits by Customer; and

i. comply with all reasonable requests of Customer resulting from any such audit.

2.3 Customer recognizes that it is in its best interest that Arista continue to update and
improve the Services for Customer. While recognizing that Arista shall be in sole
control of the priority and direction of such updates, improvements, and new features,
Customer instructs Arista to use anonymized or pseudo-anonymized versions of such
Personal Data, when useful, to help such advancement of the Services.

3. INTERNATIONAL TRANSFER

3.1 Arista and the Arista Entities have a global presence and employ cloud service
providers to manage data (pursuant to Section 4 below). Customer understands that
Arista cannot guarantee that Personal Data given to it will reside in only one country
and expressly authorizes Arista to transfer the Personal Data to locations inside and
outside of the European Economic Area in compliance with any restrictions in law or
as set forth herein.

3.2 Arista enters into the SCCs with Customer as set forth in Annex A, subject to the
following additional terms. The Parties agree that this section is not intended to
amend or modify the SCCs but represent agreed processes for complying therewith.

a. Processing Instructions. Pursuant to Clause 4(b) of the SCCs, Customer
acknowledges and agrees that the provisions of the Agreement and further
contained herein comprise the instructions for and approval to process personal
data.
b. Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 5(h) of the SCCs, Customer acknowledges and expressly agrees that (a) any Arista Entity may be retained as a Subcontractor; and (b) any Arista Entity may engage third-party Subcontractor in connection with the provision of Arista products and Services as set forth in Section 4 below.

c. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the SCCs) and the SCCs in Schedule 5, the SCCs shall prevail.

3.3 With respect to the international transfer of data out of the EU, Arista reserves the right to switch to another transfer mechanism approved by the EU Commission provided that it does not materially reduce the protections provided herein.

3.4 Customer will provide appropriate safeguards in relation to any transfer of Personal Data that it initiates pursuant to the Applicable Privacy Law(s).

3.5 Arista will provide appropriate safeguards in relation to any transfer of Personal Data that it initiates and provide any relevant Data Subject with enforceable rights and effective legal remedies pursuant to the Applicable Privacy Law(s).

4. SUBPROCESSING

4.1 Arista employs cloud service providers to manage its data including Personal Data from Customer. Customer agrees to Arista’s use of each Subcontractor, listed on Arista’s website (https://www.arista.com/en/sub-processor) which may be updated from time to time, to process Personal Data. Additionally:

a. Arista imposes substantially similar or more stringent data protection terms on any Subcontractor it engages as contained in this DPA; and

b. Arista remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error or omission of such Subcontractor.

4.2 In the event, Arista decides to engage any additional Subcontractor, Arista will notify, through the website listed in Section 4.1 above, Customer in advance of providing the Subcontractor access to Customer Personal Data. If Customer objects to the engagement of any Subcontractor on data protection grounds, then either Arista will not engage the Subcontractor to process the Personal Data controlled by Customer or Arista may elect to suspend or terminate the processing of Personal Data under the Agreement without penalty.

4.3 Customer agrees that any Arista Entity may process, subprocess, or engage an approved Subcontractor to process or subprocess Customer’s Personal Data in accordance with the terms herein. In furtherance thereof, Arista may transfer such Personal Data to any other Arista Entity.

5. DATA SUBJECTS AND COOPERATION

5.1 Arista shall reasonably cooperate to enable Customer to respond to any requests, complaints or other communications from Data Subjects and regulatory or judicial bodies relating to the processing of Personal Data under the Agreement, including
requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws. In the event that any request, complaint or communication is made directly to Arista regarding Service Personal Data, Arista shall promptly pass this onto Customer and shall not respond to such communication without Customer's express authorization.

5.2 As a Controller, Customer is responsible for providing information to Data Subjects regarding their Personal Data processed by the Cloud Services and their rights, using Customer’s own communication tools and methods. In certain cases, Customer may be able to use tools provided in the Arista Cloud Services to respond to inquiries and/or comply with a Data Subject’s request. Customer acknowledges and agrees that, in its role as Processor, Arista will not respond to Data Subject requests with respect to Customer’s provision of any service unless specifically asked to by Customer.

5.3 If Arista receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Personal Data, Arista shall not disclose any information but shall immediately notify Customer in writing of such request, and reasonably cooperate with Customer if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws. If Arista is ever not permitted under law to notify Customer, Arista will (1) seek waiver of any such requirement if possible; (2) require formal requests pursuant to legal process (such as a subpoena or court order); (3) analyze the lawfulness of any such request; and (4) challenge requests Arista deems, in its sole discretion, to be unlawful.

5.4 To the extent Arista is required under Article 28(3) GDPR, Arista will assist Customer (or its third party Controller) to comply with Articles 35 & 36 GDPR; in particular, it will promptly notify Customer if it believes that its processing of Personal Data is likely to result in a high risk to the privacy rights of Data Subjects, and upon reasonable request, will assist Customer (or the relevant Controller) to carry out data protection impact assessments and for the relevant Controller to consult where necessary with data protection authorities.

6. DATA ACCESS & SECURITY MEASURES

6.1 Arista shall ensure that any Authorized Person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for the purpose of delivering the Services under the Agreement to Arista.

6.2 Arista will implement and maintain all appropriate technical and organizational security measures to protect from Security Incidents and to preserve the security, integrity and confidentiality of Personal Data (“Security Measures”). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as to the likelihood and severity of the risk to the rights and freedoms of natural persons. At a minimum, Arista agrees to the Security Measures identified at Annex B.

6.3 Arista Cloud Services may be hosted by Subcontractors in their data centers. In such cases, there is a shared responsibility model (“SRM”) for cloud security. In this model, the Subcontractor(s) manage the security of the data centers, including physical security, environmental protection, administrative controls, technical
controls, and redundant infrastructure. Arista inherits data center security controls from the Subcontractor(s) and does not have the ability to influence their implementation or the ability to monitor or audit them. In accordance with the relevant SRM, Arista manages security of the Cloud Services application and application data, including boundary protection, host firewalls, application hardening, vulnerability assessment, data encryption, logical access control, availability monitoring, change management, and disaster recovery. Arista performs regular monitoring and evaluation of its security.

7. SECURITY INCIDENTS

7.1 In the event of a Security Incident, Arista shall promptly (and in no event later than 72 hours of becoming aware of such Security Incident) inform Customer of any actual loss or compromise of Customer Personal Data and provide written details of the Security Incident, including the type of data affected and the identity of affected person(s) as soon as such information becomes known or available to Arista.

7.2 Furthermore, in the event of a Security Incident, Arista shall:

a. provide timely information and cooperation as Customer may require to fulfil Customer's data breach reporting obligations under Applicable Privacy Laws; and

b. take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Incident and shall keep Customer up-to-date about all developments in connection with the Security Incident.

7.3 The content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at Arista's discretion, except as otherwise required by applicable laws.

8. SECURITY REPORTS

8.1 Upon request, Arista shall provide copies of relevant documentation reasonably required by Arista to verify Arista's compliance with this DPA.

9. DELETION & RETURN

9.1 Upon Customer’s reasonable request, or upon termination or expiry of this DPA, Arista shall destroy or return to Customer all Service Personal Data (including copies) in its possession or control (including any Service Personal Data processed by its Subcontractors). This requirement shall not apply to the extent that Arista is required by any applicable law to retain some or all of the Service Personal Data, in which event Arista shall isolate and protect the Service Personal Data from any further processing except to the extent required by such law.
10. **GENERAL**

10.1 The term of this DPA and the obligations placed upon Arista thereunder shall survive so long as Arista and/or its Subcontractors processes Personal Data on behalf of Customer.

10.2 This DPA may be modified unilaterally by Arista, provided that Arista notifies Customer and does not materially lower the security and data processing protections for Customer herein; otherwise this DPA may not be modified except by a subsequent written instrument signed or otherwise agreed to by both parties.

10.3 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

10.4 In the event of any conflict between this DPA and any data privacy provisions set out in any Agreement, the parties agree that the terms of this DPA shall prevail.
Annex A

STANDARD CONTRACTUAL CLAUSES
SECTION I

Clause 1
Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b) The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.
Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

   iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

   iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

   v. Clause 13;

   vi. Clause 15.1(c), (d) and (e);

   vii. Clause 16(e);

   viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.
Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to
these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy
If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data
Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing
a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data
Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers
The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union4 (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance
a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions
a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation
The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency
On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a
meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy
If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data
Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing
a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate
and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data
Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers
The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance
a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

a) The data importer has the controller’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c) The data importer shall provide, at the data exporter’s or controller’s request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.
Clause 10
Data subject rights

MODULE TWO: Transfer controller to processor

a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11
Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

PUBLIC NOTICE: After the processing of personal data by the data importer, a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   ii. refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its...
obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   ii. the laws and practices of the third country of destination— including those requiring the disclosure of data to public authorities or authorising access by such authorities— relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.
Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

**Clause 16**

*Non-compliance with the Clauses and termination*

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

c) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

d) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU)
2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18
Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b) The Parties agree that those shall be the courts of Ireland.

c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d) The Parties agree to submit themselves to the jurisdiction of such courts.
APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Data exporter(s):
1. Name: Customer as set forth in the Agreement
Address:
Contact person’s name, position and contact details:
Activities relevant to the data transferred under these Clauses:
Signature and date: …
Role (controller/processor): controller or processor

Data importer(s):
1. Name: Arista
Address:
Contact person’s name, position and contact details:
Activities relevant to the data transferred under these Clauses:
Signature and date: …
Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred
1) Controller’s employees and/or controller’s end users of the Products and Services of the Agreement

Categories of personal data transferred
1) Contact Information, user device IDs and location data as Controller sets up through the Services

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
1) N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
ongoing/continuous
Nature of the processing

   Storage and evaluation to provide the Services as set forth in the Agreement

Purpose(s) of the data transfer and further processing

   To provide the Services as set forth in the Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

   Duration of the Agreement and any subsequent similar agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

   As described in the DPA and Agreement

C. COMPETENT SUPERVISORY AUTHORITY

   MODULE TWO: Transfer controller to processor
   MODULE THREE: Transfer processor to processor

   Identify the competent supervisory authority/ies in accordance with Clause 13 the Data Protection Commission of Ireland.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

   See Annex B of the DPA

ANNEX III – LIST OF SUB-PROCESSORS

   NOT REQUIRED DUE TO CLAUSE 9(A) GENERAL OPTION
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):**

The technical and organizational security measures set out in Annex B to the DPA to which these EU Standard Contractual Clauses are attached detail the measures to be implemented in accordance with this Appendix 2

**On behalf of the data exporter:**

**Customer**

Signature: ________________________________

Printed Name (written out in full): ________________________________

Position/Title: ________________________________

Address: ________________________________

Date: ________________________________

**On behalf of the data importer:**

**Arista Networks**

Signature: ________________________________

Printed Name (written out in full): ________________________________

Position/Title: ________________________________

Address: ________________________________

Date: ________________________________
Annex B

Technical and Organisational Security Measures

This Annex B sets out a description of the minimum technical and organisational security measures that Arista implements.

Arista takes information security seriously and this approach is followed through in its processing and transfers of personal data. This information security overview applies to Arista’s corporate controls for safeguarding personal data which is processed and transferred amongst Arista’s group companies. Arista's information security program enables the workforce to understand their responsibilities. Some customer solutions may have alternate safeguards outlined in the applicable statement of work as agreed with each customer.

Security Practices

Arista has implemented corporate information security practices and standards that are designed to safeguard Arista’s corporate environment and to address business objectives across the following areas:

1) information security
2) system and asset management
3) development, and
4) governance.

These practices and standards are approved by Arista's executive management and are periodically reviewed and updated where necessary.

Arista shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. Key policies should be reviewed at least annually.

Organizational Security

It is the responsibility of the individuals across Arista’s organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, Arista’s Information Security (“IS”) function is responsible for the following activities:

1. Security strategy – the IS function drives Arista’s security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities, and manages contract security requirements.

2. Security engineering – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.

3. Security operations – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.
4. **Forensic investigations** – the IS function works with Security Operations, Legal, Global Privacy Office and Human Resources to carry out investigations, including eDiscovery and eForensics.

5. **Security consulting and testing** – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

### Asset Classification and Control

Arista’s practice is to track and manage key information and physical, software and logical assets. Examples of the assets that Arista might track include:

- information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information
- software assets, such as identified applications and system software
- physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

### Employee Screening, Training and Security

1. **Screening/background checks**: Where reasonably practicable and appropriate, as part of the employment/recruitment process, Arista shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to Arista’s networks, systems or facilities.

2. **Identification**: Arista shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other Arista entities or customers for whom the employee is providing services.

3. **Training**: Arista’s annual compliance training program includes a requirement for employees to complete a data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.

4. **Confidentiality**: Arista shall ensure its employees are legally bound to protect and maintain the confidentiality of any personal data they handle pursuant to standard agreements.

### Physical Access Controls and Environmental Security

1. **Physical Security Program**: Arista shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the
extent reasonably practicable. Arista’s security team works closely with each site to
determine appropriate measures are in place to prevent unauthorized persons from
gaining access to systems within which personal data is processed and continually
monitor any changes to the physical infrastructure, business and known threats. They
also monitor best practice measures used by others in the industry and carefully select
approaches that meet both uniqueness in business practice and expectations of Arista.
Arista balances its approach towards security by considering elements of control that
include architecture, operations and systems.

2. **Physical Access controls:** Physical access controls/security measures at Arista’s
facilities/premises are designed to meet the following requirements:

   a) access to Arista’s buildings, facilities and other physical premises shall be
controlled and based upon business necessity, sensitivity of assets and the
individual’s role and relationship to Arista. Only personnel associated with Arista
are provided access to Arista’s facilities and physical resources in a manner
consistent with their role and responsibilities in the organization;

   b) relevant Arista facilities are secured by an access control system. Access to such
facilities is granted with an activated card only;

   c) all persons requiring access to facilities and/or resources are issued with
appropriate and unique physical access credentials (e.g. a badge or key card
assigned to one individual) by the IS function. Individuals issued with unique
physical access credentials are instructed not to allow or enable other individuals
to access the Arista’s facilities or resources using their unique credentials (e.g. no
“tailgating”). Temporary (up to 14 days) credentials may be issued to individuals
who do not have active identities where this is necessary (i) for access to a
specific facility and (ii) for valid business needs. Unique credentials are non-
transferable and if an individual cannot produce their credentials upon request
they may be denied entry to Arista’s facilities or escorted off the premises. At
staffed entrances, individuals are required to present a valid photo identification or
valid credentials to the security representative upon entering. Individuals who
have lost or misplaced their credentials or other identification are required to enter
through a staffed entrance and be issued a temporary badge by a security
representative;

   d) employees are regularly trained and reminded to always carry their credentials,
store their laptops, portable devices and documents in a secure location
(especially while traveling) and log out or shut down their computers when away
from their desk;

   e) visitors who require access to Arista’s facilities must enter through a staffed and/or
main facility entrance. Visitors must register their date and time of arrival, time of
leaving the building and the name of the person they are visiting. Visitors must
produce a current, government issued form of identification to validate their
identity. To prevent access to, or disclosure of, company proprietary information
visitors are not allowed un-escorted access to restricted or controlled areas;

   f) select Arista facilities use CCTV monitoring, security guards and other physical
measures where appropriate and legally permitted;

   g) locked shred bins are provided on most sites to enable secure destruction of
confidential information/personal data;
h) for Arista’s major data centres, security guards, UPS and generators, and change control standards are available;

i) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

Change Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

Security Incidents and Response Plan

1. **Security incident response plan**: Arista maintains a security incident response policy and related plan and procedures which address the measures that Arista will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized acquisition of personal data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. **Response controls**: Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the Arista’s IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

Data Transmission Control and Encryption

Arista shall, to the extent it has control over any electronic transmission or transfer of personal data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. In particular, Arista shall:

1. implement industry-standard encryption practices in its transmission of personal data, including standard encryption practices from the National Institute of Standards and Technology (NIST). Industry-standard encryption methods used by Arista includes Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);

2. if technically feasible, encrypt all personal data, including, in particular any sensitive personal data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by Arista. The
Arista's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document;

3. for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including Arista’s core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

System Access Controls

Access to Arista’s systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted so as to prevent access from unauthorised individuals. Such procedures include:

1. admission controls (i.e. measures to prevent unauthorized persons from using data processing systems):
   a) access is provided based on segregation of duties and least privileges in order to reduce the risk of misuse, intention or otherwise;
   b) access to IT systems will be granted only when a user is registered under a valid username and password;
   c) Arista has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;
   d) mandatory password changes on a regular basis;
   e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;
   f) data and user classification determines the type of authentication that must be used by each system;
   g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. access controls (i.e. measures to prevent unauthorised access to systems):
   a) access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);
   b) adjustment of access authorizations in case of changes to the working area, or in case an employee’s employment is terminated for any reason;
   c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question;
d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

**Data Access Control**

Arista applies the controls set out below regarding the access and use of personal data:

1. personnel are instructed to only use the minimum amount of personal data necessary in order to achieve Arista’s relevant business purposes;

2. personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;

3. third party use of personal data is governed through contractual terms and conditions between the third party and Arista which impose limits on the third party’s use of personal data and restricts such use to what is necessary for the third party to provide services.

**Separation Control**

Where legally required, Arista will ensure that personal data collected for different purposes can be processed separately. Arista shall also ensure there is separation between test and production systems.

**Job Control**

Arista shall process personal data in accordance with the applicable services agreement between Arista and data exporter and in accordance with the instructions of the data exporter. The following controls will be implemented by the Arista:

1. personal data is processed only to the extent necessary for contractual performance;

2. personnel are subject to a written obligation of confidentiality;

3. diligent selection of (sub)processor and other service providers;

4. third party use of personal data is governed through contractual terms and conditions between the third party and Arista which impose limits on the third party’s use of personal data and restricts such use to what is necessary for the third party to provide services;

5. clear instructions to (sub)processors on security measures for protecting privacy including the appropriate technical and organizational measures to safeguard the personal data to the same or higher level of protection as provided by Arista;

6. ongoing monitoring of (sub)processor’s activities.
Availability Control

Arista protects personal data against accidental destruction or loss by following these controls:

1. personal data is retained in accordance with customer contract or, in its absence, Arista’s record management policy and practices, as well as legal retention requirements;

2. hardcopy personal data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;

3. electronic personal data is given to Arista’s IT Asset Management team for proper disposal;

4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

Data Input Control

Arista has, where appropriate, measures designed to check whether and by whom personal data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded.

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the Arista environment. Based on risk to Arista’s business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

Compliance

The information security, legal, privacy and compliance departments work to identify regional laws and regulations that may be applicable to Arista. These requirements cover areas such as, intellectual property of Arista and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements.

Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.