DATA PROCESSING AGREEMENT

This Data Processing Agreement including its attachments (the "**Agreement**", "**Data Processing Agreement**", or "**DPA**") is entered into by and between Supplier ("**Supplier**" or "**Processor**") and **Ingram Micro Inc.** having its registered office at 3351 Michelson Dr. Irvine, California 92612, ("**Ingram Micro**" or "**Controller**"). Supplier and Ingram Micro are hereinafter also referred to individually as a "**Party**" and collectively as the "**Parties**".

WHEREAS:

A. Controller and Processor have entered into a Master Service Agreement as defined below, by which Processor provides Services to Controller;

B. Processor will Process Personal Data on behalf of Ingram Micro in the course of providing the Services to Controller pursuant to the Master Service Agreement;

C. The Parties wish to reflect the Parties' agreement regarding the Processing of Personal Data in compliance with the relevant Data Protection Laws and Regulations and more specific in compliance with the General Data Protection Regulation;

D. Regarding the Processing of Personal Data, the provisions of this Data Processing Agreement supersede all previous understandings and agreements between the Parties.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

"Attachment" means each annex, exhibit, schedule or other attachment to this Data Processing Agreement which forms part of the Agreement;

"**Approved Subcontractor**" means a subcontractor or Sub-processor that Controller has provided written consent to Processor to use as a subcontractor or Sub-processor.

"Data Subject" means any identified or identifiable person or legal entity (if the case may be under the applicable legislation) to whom Personal Data relates; an identifiable 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 the physical, psychological, genetic, mental, economic, cultural and/or social identity of that person;

"Data Controller" or "Controller" means the legal person which alone or in conjunction with others, determines the purposes and means of the Processing of Personal Data;

"Data Protection Laws and Regulations" means all applicable laws, directives, ordinances, rules, regulations etc. including but not limited to European or local country laws and regulations, such as the GDPR, and to the extent applicable, the data protection or privacy laws of any country applicable to the Processing of Personal Data under this Agreement and the MSA;

"Data Security Breach" means any incident involving the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of or access to Personal Data, under this Agreement;

“Data Transfer” or **“Transfer”** means any cross-border communication of Personal Data regardless of the format, any storage of Personal Data on data-bases hosted in different countries, any access to Personal Data hosted in a different country or the use of Personal Data by Third Parties;

“GDPR” or **“General Data Protection Regulation”** means the EU General Data Protection Regulation 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, and repealing Directive 95/46/EC;

“EEA” means the European Economic Area which consists of all countries of the European Union, Liechtenstein, Norway and Iceland;

“MSA” or **“Master Service Agreement”** means the main agreement for the provision of Services between Controller and Processor;

“Personal Data” means any information relating to an identified or identifiable natural person or legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), received and processed by Processor on behalf of and for Controller or its Clients under this Agreement and in course of providing the Services;

“Processing”, “Process” or “Data Processing” means any operation or any set of operations concerning Personal Data, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, dissemination, disclosure by means of transmission, distribution or otherwise making available in any other form, merging, linking, as well as restriction, erasure or destruction of data;

“Data Processor” or **“Processor”** means the entity which Processes Personal Data on behalf of the Controller;

“Services” means all Services Processor provides as agreed to by the Master Service Agreement;

“**Service Employee**” means any agent or employee of Supplier or its Approved Subcontractors:

“Standard Contractual Clauses” means the contractual clauses pursuant to the European Commission’s decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council;

“Sub-processor” means any data processor engaged by Processor in the course of providing the Services;

“Supervisory Authority” means an independent public authority established in a particular country responsible for monitoring the compliance with the Data Protection Laws and Regulations within such country, in order to protect the fundamental rights and freedoms of natural persons in relation to processing; and

“Third Party” means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, or Processor.

2. GENERAL

2.1 If Supplier is provided access to any Personal Data, Supplier agrees to maintain an appropriate data protection and privacy program in compliance with this Agreement which is incorporated in the MSA by this reference. Supplier agrees and acknowledges that Supplier, its Approved Subcontractors and Service Employees will abide at all times by the terms set form in this Agreement, which may be updated from time to time in Ingram Micro's sole discretion.

2.2 The Parties shall at all times comply with the applicable data protection legislation and privacy laws, including without limitation the EU Privacy Directive and the General Data Protection Regulation, and will not by any act or omission put the other Party in breach of its legal obligations under the applicable legislation and in connection with this Agreement; The Parties acknowledge and agree that with regard to the Processing of Personal Data, Ingram Micro is the Data Controller and Service Provder is the Data Processor.

The subject-matter of Processing of Personal Data by the Processor is the performance of the Services pursuant to the Master Service Agreement.

Processor will Process Personal Data for Controller in accordance with this Data Processing Agreement, the applicable Data Protection Laws and Regulations and with Controller's written instructions in relation to the Processing of Personal Data as part of providing the Services. Processor agrees and certifies to use the Personal Data strictly for the purposes defined by Controller and for no other purpose. Processor shall at all times treat Controller's Personal Data under the MSA and this DPA as confidential information, subject to the provisions set forth in clause 4 of this Agreement.

2.3 Processor and Controller will timely provide each other with all necessary information regarding the Processing of Personal Data to enable compliance with the relevant Data Protection Laws and Regulations.

3. PROCESSING OF PERSONAL DATA AND CROSS-BORDER DATA TRANSFER

3.1 **Attachment 1** contains an overview of categories of Data Subjects, categories of Personal Data and the purposes of Processing of Personal Data, under this Data Processing Agreement. Processor shall Process and use the Personal Data solely for the purposes defined by the Controller as set out in **Attachment 1.** The Parties agree that reasonable amendments to Attachment 1 might take place upon mutual agreement by the Parties from time to time as necessary to meet legal and data protection requirements.

3.2 Processor will only Process Personal Data on behalf of and in accordance with Ingram Micro's documented instructions in the course of providing the Services under the MSA or to comply with legal obligations to which Processor or its affiliated companies are subject. For the avoidance of doubt, Controller will ensure that its instructions for the Processing of Personal Data shall comply with the applicable Data Protection Laws and Regulations. If however, at any time during the execution of this Agreement and the MSA, Controller's instructions appear in any way to be unlawful or non-compliant with the applicable legislation, Processor shall without undue delay notify this to Controller and wait for further instructions.

3.3 In the event a legal requirement prevents Processor from complying with Controller's instructions or requires Processor to Process the Personal data for a particular purpose or to disclose the Personal Data to a Third Party, Processor shall promptly inform Controller in writing of the relevant legal requirement before carrying out the relevant Processing activities and co-operate with Controller regarding the manner of such disclosure. In case of any disclosure based on a legal obligation Processor will verify the request and the identity of the person making the request.

3.4 Processor shall not perform cross-border Transfers outside the EEA, disclose or otherwise permit access to the Personal Data to any Third Party for any purpose, without Controller's prior written consent, even if the Transfer, the disclosure or the access permission are strictly necessary for the performance of the Services and Processor's compliance with the terms of this Agreement and the MSA or in order to comply with a legal obligation.

3.5 The Parties agree and certify that any disclosure, access or Data Transfer outside the EEA, of Controller's Personal Data under this Agreement and the MSA, to the Processor, any Sub-processors or Third Parties, will be performed in compliance with the applicable Data Protection Laws and Regulations, the provisions set forth in this Data Processing Agreement and only upon implementing a legally valid data transfer safeguard mechanism as provided under the GDPR such as by entering into the Standard Contractual Clauses, which is incorporated, as needed, into this Agreement in Attachment 3.

3.6 For the avoidance of doubt, subject to the provisions set forth in clause 3.4 and 3.5, Processor warrants and represents that the Personal Data, transferred to and Processed outside the European Economic Area, on behalf of Controller, will be subject to the highest level of security and protection relevant to the nature of the Processing and the type of Personal Data, and such Processing and Data Transfer will be performed with full and strict compliance with Controller's instructions and the applicable Data Protection Laws and Regulations.

For the Processing of Personal Data outside the EEA, Processor will provide Controller with an overview in writing of the countries in which the Personal Data is Processed or transferred to and in what way Processor complies with the applicable Data Protection Laws and Regulations.

3.7 Upon Controller's request, Processor shall provide Controller with reasonable cooperation and assistance needed to fulfill Controller's obligations under the applicable Data Protection Laws and Regulations and to carry out data protection impact assessments, to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide reasonable assistance to Controller in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks under this Agreement, to the extent required under the applicable Data Protection Laws and Regulations.

4. CONFIDENTIALITY

4.1 Processor shall keep strictly confidential the Personal Data it Processes for the purpose of this Data Processing Agreement and will take all measures necessary to ensure the confidentiality of the Personal Data. Processor shall refrain from disclosing, using, exploiting or Processing in any way any and all Personal Data for any purposes or activities other than those specifically authorized in this Data Processing Agreement.

4.2 Processor shall ensure that access to the Personal Data is limited to those of its employees or its subcontractors who have a need to know and must have access to the Personal Data in order to provide the Services, and only for the purposes set forth in this Data Processing Agreement. Processor shall ensure that all employees and other individuals engaged in the Processing of Personal Data are aware of the applicable Data Protection Laws and Regulations, are informed of the confidential nature of the Personal Data, comply with the obligations and restrictions set forth herein and are subject to written confidentiality obligations. Processor warrants and represents to the Controller that such confidentiality obligations of its personnel shall survive the termination of their employment with Processor. Processor certifies that its employees shall not Process the Personal Data other than for the purposes as described in this Data Processing Agreement. Processor shall only disclose Personal Data to Third Parties with the prior written consent of Controller or as otherwise specifically agreed in this Data Processing Agreement.

The confidentiality obligations set forth under this Section 4 shall survive for five year(s) after the expiration or earlier termination of this Data Processing Agreement or the MSA and will continue to apply to all Personal Data that the Processor has the right to retain as required by applicable laws and only to the extent and for such period as required by the applicable laws and in order to defend its interests.

4.3 The confidentiality as described in this paragraph does not apply in case of a legal obligation to disclose the Personal Data, or when the data is required to be disclosed to any government authority, such as without limitation the Supervisory Authority pursuant to and required by any applicable law or court order and after giving prompt written notice to the Controller prior to such disclosure in order to allow him to limit if possible the disclosure.

5. SECURITY OF PERSONAL DATA

5.1 Processor shall take, maintain and if required alter all necessary and appropriate technical and organizational security measures to ensure the security, availability, confidentiality and integrity of its computers, other information systems and Services, and to protect Personal Data under this Agreement, against accidental, unauthorized or unlawful destruction, disclosure, coping, use, loss, alteration, or access and all other forms of unlawful or unauthorized Processing in accordance with the applicable Data Protection Laws and Regulations. Processor shall ensure that its systems (including security software and connections) are in compliance with the applicable Data Protection Laws and Regulations, Controller's policies and the best practice and industry standards, in order to ensure the privacy by design required by Data Protection Laws and Regulations.

5.2 Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the nature of Personal Data as well as the risk and severity for the rights and freedoms of natural persons, Processor warrants that its security measures ensure a level of security appropriate to the risks presented by the Processing of Personal Data. Processor shall maintain such security measures and comply with the Data Protection Laws and Regulations for as long as it is Processing the Personal Data, and this Agreement and the MSA are not expired or terminated.

5.3 The technical and organizational security measures Processor has implemented are specified in **Attachment 2** to this Data Processing Agreement. Parties will periodically evaluate the security measures and if required mutually amend **Attachment 2.**

6. AUDITS

6.1 Processor agrees to provide Controller at least once a year with a copy of any third-party audit or report regarding the technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data. Upon signing the Data Processing Agreement, Processor will provide Controller with a copy of its most recent third-party audits or certifications.

6.2 Controller has the right to audit or have an independent third-party auditor, inspector, regulator, and other representative, as Controller may from time to time designate in writing, to perform an audit on its behalf in order to audit Processors' compliance with its obligations under the Data Processing Agreement and the applicable Data Protection Laws and Regulations. Processor shall provide Controller, upon written request, with all information necessary to demonstrate compliance with Processor’s obligations under this Data Processing Agreement. Processor shall ensure full cooperation in the performance of the audit and will grant the auditor access to its premises in which Processor is providing Services to Controller, to relevant Processor Personnel and to databases, computer systems and records and any and all information relating to the Services and relevant for the audit.

6.3 Controller may perform such audits no more than once in any calendar year unless Controller has a reasonable suspicion of a breach or potential breach of this Data Processing Agreement by Processor, in which event Controller may perform an audit whenever required. Controller shall inform Processor prior to any inspection. Controller undertakes to carry out any inspection during normal working hours, at a mutually agreed upon date and time, and without interfering with the course of Processor’s business.

6.4 Recommendations and/or required alterations following from the audits will be assessed and applied by Processor after having consulted Controller.

6.5 In the event that the results of the audit show that Processor does not comply with its obligations under the Data Processing Agreement the Processor shall bear the costs of the audit.

6.6 In case of an investigation by any other competent authority Processor will ensure all reasonable cooperation and inform Controller immediately and shall not disclose any Personal Data without a prior written notification to Controller. Parties shall consult with each other on how to act regarding the investigation.

7. SECURITY BREACHES AND NOTIFICATION

7.1 If the Processor becomes aware of any incident involving the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of or access to Controller’s Personal Data, the Processor shall notify the Controller without undue delay about the Data Security Breach or security incident related to the Processing of Personal Data under this Agreement and the MSA. Processor shall maintain security incident management policies and procedures. Processor shall immediately investigate and provide the Controller with sufficient information related to the Data Security Breach in order to allow him to meet any legal obligation to report or inform Data Subjects or the Supervisory Authority of the Data Security Breach under the applicable Data Protection Laws and Regulations. Such information is specified in Attachment 3 and should include the nature of the Data Security Breach, the categories of Data Subjects affected, the categories and numbers of Personal Data records concerned, the contact details of the Processor’s Data Protection Officer (if such is required to be appointed by law) and describe the likely consequences of the Data Security Breach and the measures taken or proposed to be taken to address such Data Security Breach.

7.2 In case of a security incident Processor will immediately take adequate measures to mitigate the consequences of the incident and to prevent future incidents. Processor will ensure full cooperation in order to enable the Controller to comply with its legal obligation to notify Data Security Breaches and to inform Data Subjects and the Supervisory Authority within the time frame provided in the applicable Data Protection Laws and Regulations.

7.3 In case of a security incident on the part of the Processor which leads to the legal obligation for Controller to notify about the Data Security Breach to the relevant Data Subject or to any Supervisory Authority, Processor will bear all costs involved, including reimbursing Controller for all internal costs and labor.

8. DATA SUBJECTS REQUESTS

8.1 Processor shall promptly notify Controller if it receives a request from a Data Subject to exercise its rights of access, rectification, amendment, restriction of Processing or deletion ("right to be forgotten'), data portability, objection to the Processing of that person's Personal Data or any other Data Subject request, under any of the applicable Data Protection Laws and Regulations. Processor will not respond to any such Data Subject request without Controller's prior written consent and in accordance with Controller's instructions, except to confirm that the request relates to Controller.

Taking into account the nature of the Processing, Processor shall implement appropriate technical and organizational measures, for the fulfilment of Controller's obligations to respond to Data Subject requests related to the exercise of their rights under the applicable Data Protection Laws and Regulations.

8.2 Processor shall provide Controller with all reasonable cooperation and assistance in order to enable Controller to comply with its legal obligations in relation to the handling of Data Subject requests, within the statutory time limits, to the extent that the Processor is legally permitted to do so and provided that such Data Subject Requests are exercised in accordance with the applicable Data Protection Laws and Regulations.

9. SUB-PROCESSOR

9.1 Processor shall not subcontract any of its Processing operations regarding Controller's Personal Data without the express prior written consent of Controller which consent could be granted or withhold at Controller's sole discretion. For any proposed Sub-processor, Processor shall disclose to Controller the full legal name and company registration number of such Sub-processor or Sub-processor Affiliate and the geographic location(s) at which the proposed Sub-processor will perform the Processing operations regarding the Personal Data, and details of the volume of records and nature of the Processing that will take place.

9.2 In the event Controller provides its approval on such Sub-processor, upon Controller's request Processor hereby agrees to provide Controller with a copy of the sub-processing agreement with its Sub-processor. Processor shall promptly inform the Controller of any changes related to the Sub-processor which could impact the Processing of the Personal Data. Processor shall obtain Controller's prior written consent to any such changes, which consent shall not be unreasonably withheld.

9.3 Processor shall only subcontract its Processing operations regarding the Personal Data by way of a written agreement signed between the Processor and the Sub-processor which imposes and requires the

Sub-processor to comply with the same obligations and restrictions as the one imposed on the Processor by the applicable Data Protection Laws and Regulations and this Data Processing Agreement. Processor shall remain fully responsible for any acts and omissions of its Sub-processors to the same extent as if such acts or omissions were performed by the Processor. In case the Processor subcontracts the Processing operations regarding the Personal Data to a Sub-processor without the express written consent of the Controller and/or in non-compliance with the Controller's objection, such subcontracting will be considered a material breach and the Controller will have the right to terminate this Data Processing Agreement and the MSA.

10. ACCESS TO PERSONAL DATA

10.1 The Personal Data belongs exclusively to Controller. Processor warrants full and continuous access to the Personal Data, also in case of any conflict between the Parties for whatever reason.

10.2 Processor shall ensure that its personnel engaged in the Processing of Personal Data under this Agreement and the MSA, have received appropriate training on their responsibilities, necessary to comply with the terms of this Agreement. Processor shall take commercially reasonable steps to ensure the reliability of any personnel engaged in the Processing of Personal Data. Processor shall ensure that the access to Personal Data is limited to those personnel who require such access to perform the Services under this Agreement and the MSA. Processor certifies to have appointed a data protection officer where such appointment is required by the applicable Data Protection Laws and Regulations.

11. RETURN AND DELETION OF CUSTOMER DATA

11.1 Processor will retain the Personal Data for a duration as instructed by the Controller. Parties can mutually agree to retention periods in Attachment 1. Processor warrants to return or, to the extent allowed by the applicable laws and in accordance with Controller's instructions and the terms of this Agreement, delete and destroy all Personal Data and any copies of such data after the retention period has lapsed.

11.2 Upon Controller's request, expiration or earlier termination of this Agreement, Processor shall promptly and in any event within thirty (30) days of the date of cessation of any Services involving the Processing of Controller's Personal Data (the "Cessation Date"), return to Controller, or to any Third Party specified in writing by the Controller, or delete and procure a certification of destruction of all copies of Controller's Personal Data that might be in their possession. The return of Controller's Personal data and all its copies in Processor's possession shall be completed by secure file transfer in such format as is reasonably requested by Controller to Processor.

11.3 The Processor may retain Controller's Personal Data to the extent required by the applicable laws and only to that extent and for such period as required by the applicable laws. Notwithstanding the above, Processor may retain Controller's Personal Data exclusively provided that Processor shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

12. INDEMNIFICATION AND LIABILITY

12.1 Processor shall be held liable for all damages, losses, liabilities, expenses and costs incurred by

Controller in the event Processor breaches and fails to comply with the applicable Data Protection Laws and Regulations and the terms and conditions laid down in this Data Processing Agreement, in accordance with the provisions on liability and damages laid down in the Master Service Agreement.

12.2 Processor shall indemnify and hold harmless the Controller and its clients from any liability, losses, claims, penalties, damages, costs and expenses (including attorney's fees and court costs) of whatever nature arising out of any claims, actions, proceedings or settlements resulting from (i) the breach or non-compliance of Processor with the terms and conditions of this Data Processing Agreement and/or with the applicable Data Protection Laws and Regulations or (ii) the negligence or willful misconduct of the Processor, its Sub-processor, employees or authorized representatives.

13. TERMINATION

13.1 The Data Processing Agreement will be effective as of the date of the last signature (the "Effective Date") and shall remain in force during the term of the MSA. This Data Processing Agreement will terminate automatically with the termination or expiry of the MSA.

13.2 In the event that Processor fails to comply with this Data Processing Agreement, Controller may terminate the Data Processing Agreement and the MSA, effective immediately, at its sole discretion, upon written notice to Processor without liability or further obligation to Controller and without prejudice to any other remedies under this Data Processing Agreement, at law or in equity.

14. MISCELLANEOUS

14.1 In the event of changes in the Services or applicable Data Protection Laws and Regulations which will affect the Processing of the Personal Data and requires the amendment of the Data Processing Agreement in order for the Parties to be able to address the requirements and comply with the applicable laws, the Parties will consult with each other in good faith in order to amend the Data Processing Agreement. Any amendments to this Data Processing Agreement can solely be made in writing by duly authorized representatives of the Parties.

14.2 The Parties can at any time mutually agree on amendments to the Attachments in writing and by adding a new version number to the Attachment.

14.3 If any provision of this Data Processing Agreement is found by any court or administrative body of competent jurisdiction to be void, invalid, illegal or otherwise unenforceable, all other terms and provisions of this Data Processing Agreement shall nevertheless remain in full force and effect, and the invalidity or unenforceability of such provision will not adversely affect the enforceability of any other provision of this Data Processing Agreement. The Parties agree that in the place of the invalid provision, a legally binding provision shall apply which comes closest to what the Parties would have agreed if they had contemplated the partial invalidity.

14.4 In the event of a conflict between any of the terms of this Data Processing Agreement and its Attachments, the terms of this Data Processing Agreement shall prevail. Notwithstanding the foregoing, any conflict between the provisions of this Data Processing Agreement and the Standard Contractual Clauses set forth in Attachment 4, shall be resolved in favor of such Standard Contractual Clauses. In case of any contradiction and inconsistency between the provisions of this Data Processing Agreement and the provisions set forth in the MSA, the provisions that are more protective of Personal Data shall prevail.

The Master Service Agreement shall continue to apply for all matters and topics not covered by this Data Processing Agreement.

14.5 The titles in this Agreement and the Attachments are for reference purposes only and shall not affect in any way whatsoever the meaning or interpretation of this Data Processing Agreement.

15. APPLICABLE LAW AND JURISDICTION

15.1 This Data Processing Agreement shall exclusively be governed by and construed in accordance with the laws of the California, USA.

15.2 Any dispute, controversy or claim arising out of or in connection with this Data Processing Agreement or the breach, termination or invalidity thereof shall be settled and submitted to the competent courts of California, USA.

Attachment 1

A. Categories of Data Subjects

Processor will process Personal Data regarding the following categories of Data Subjects:

Ingram Micro employees, customers, resellers, vendors, contractors, and/or business partners.

B. Categories of Personal Data

Personal Data processed by Processor may include:

Name, personal address, personal email address, personal phone number, purchase information, job title, business address, business email address, business phone number, financial account information.

C. Purposes of Processing Personal Data

The Personal Data will in any event be processed for the following purposes:

Strictly to provide the Services and/or products in accordance with the MSA and applicable Data Protection Laws and the Ingram Micro's (as data controller) instructions.

D. Cross-Border Data Transfer and Data Processing

The Personal Data will be processed and transferred to the following countries outside the EEA:

As approved by Ingram Micro

E. Sub-processors

Processor has contracted the following Sub-processors:

As approved by Ingram Micro

F. Retention Period

For the duration of the MSA and as mutually agreed upon by Ingram Micro and Supplier

G. Contact details

The contact person regarding this Data Processing Agreement is:

Controller:
Name: Aaron Mendelsohn: Ingram Micro Data Protection Officer
E-mail address: Aaron.Mendelsohn@ingrammicro.com and Privacy@ingrammicro.com

Processor:

Name and E-mail address: Supplier contact as specified in the MSA or otherwise communicated by Processor

Attachment 2

Description of the organizational and technical security measures of the Processor in order to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and all other forms of unlawful Processing in accordance with applicable Data Protection Laws and Regulations. Supplier, its Approved Subcontractors and Service Employees will abide at all times by the terms set forth in Ingram Micro's Cybersecurity Agreement, which may be updated from time to time and can be found at https://corp.ingrammicro.com/en-us/become_partner/become_supplier.

Attachment 3:

STANDARD CONTRACTUAL CLAUSES

pursuant to the COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

Name of the data exporting organisation: Ingram Micro Inc.

Address: 3351 Michelson Dr, Irvine, California 92612

Incorporated under the laws of Delaware

(the data **exporter**)

Name of the data importing organisation: Supplier (as identified in the MSA)

(the data **importer**)

each a “**party**”; together “**the parties**”,

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)[1] 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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);.

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

Docking clause

Not used

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.

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 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. 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 Union[2]

.

(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.

Clause 9
Use of sub-processors

a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 (thirty) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

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.[3] 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 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.

Clause 10
Data subject rights

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.

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.

b) In case of 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

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

a) 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.

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;[4]

(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).

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. 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 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.

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.).

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.

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 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.

d) 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.

e) 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

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 Bulgaria.

Clause 18

Choice of forum and jurisdiction

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 Bulgaria.

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: Data Processing

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Ingram Micro Inc.

   Address: 3351 Michelson Dr., Irvine, California 92612

   Contact person's name, position and contact details: Aaron Mendelsohn, Chief Data Privacy Officer, aaron.mendelsohn@ingrammicro.com

   Activities relevant to the data transferred under these Clauses: Services under the MSA

   Role (controller/processor): controller

Data importer(s):

1. Name: Supplier (as identified in the MSA)

   Activities relevant to the data transferred under these Clauses: Services under the MSA

   Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

1. Categories of Data Subjects whose Personal Data is transferred: such Data Subjects whose transferred Personal Data is strictly required by the Service Provider (as data importer) to provide the services and/or products;
2. Categories of transferred Personal Data: such transferred Personal Data as is strictly required by the Service Provider (as data importer) to provide the services and/or products;
3. Special categories of Personal Data transferred (if applicable): such special categories of transferred Personal Data as is strictly required by the Service Provider (as data importer) to provide the services and/or products.
4. Frequency of the transfer: regular as required in connection with the provision and receipt of the services and/or products;
5. Nature and purpose(s) of the data transfer and further Processing: strictly to provide the services and/or products in accordance with applicable Data Protection Laws and the Ingram Micro's (as data exporter) instructions;
6. The period for which the transferred Personal Data will be retained, or if that is not possible, the criteria used to determine that period: for no longer than is necessary to provide the services and/or products (unless otherwise agreed with Ingram Micro); and
7. Subject matter, nature and duration of the Processing in relation to any transfers to (sub-)processors: as per 5 above

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: Bulgaria

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

See Attachment 2.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: As approved by Ingram Micro