DATA PROCESSING ADDENDUM

This Data Processing Addendum, including the applicable schedules (collectively, the "Addendum"), supplements and is incorporated by reference into, the Harman International Industries, Incorporated Terms and Conditions for Indirect Procurement ("Terms and Conditions") entered between Harman International Industries, Incorporated, or one of its affiliated companies ("Buyer") and [insert Seller legal entity name] ("Seller") (hereinafter, Buyer and Seller are, at times, jointly referred to as the "Parties"). This Addendum shall become effective as of the effective date of the Terms and Conditions.

RECITALS

WHEREAS, in connection with the Terms and Conditions, Seller Processes, on Buyer's behalf, Personal Data concerning Buyer's prospective, current, and/or former employees and/or other Data Subjects;

WHEREAS, Buyer seeks to obtain written assurances from Seller that it is Processing Personal Data in accordance with all Applicable Data Protection Laws;

NOW THEREFORE, for good and valuable consideration, the adequacy and sufficiency of which hereby are acknowledged, the Parties agree as follows.

AGREEMENT

I. Definitions

A. "Adequacy Determination" means a final determination by a governmental authority authorized by Applicable Data Protection Laws to make such a determination that the laws of a third country provide an adequate level of protection for Personal Data when that Personal Data is transferred from the jurisdiction of the governmental authority to the third country.

B. "Applicable Data Protection Laws" means any applicable law, regulation, legislation, directive, or code of conduct or other legally binding enactment applicable to the processing of Harman Personal Data.

C. "Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

D. "Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

E. "Data Subject" means the natural person who is the subject of Personal Data.

F. "Discover," with respect to a Security Incident, means knowledge by any member of Seller's workforce — other than the person responsible for the Security Incident — that the Security Incident has occurred.

G. "Personal Data" means any information received by Seller from, or created or received by Seller on behalf of, Buyer, relating to an identified or identifiable natural person. An "identifiable natural person" is one who can be identified, directly or indirectly, in

particular, by reference to an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person.

H. "Process", "Processes" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, including the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, transfer, dissemination by means of transmission, distribution or otherwise making available, merging, linking as well as blocking, erasure or destruction.

I. "Required By Law" means that a statute, regulation, court order, or legal process, enforceable in a court of law, mandates the conduct.

J. "Security Incident" means (1) the suspected or successful loss, or unauthorized access to, or use, disclosure, acquisition, modification, or destruction, of Trigger Data; or (2) interference with system operations in an information system containing Trigger Data which interference materially compromises the confidentiality, integrity, or availability of Trigger Data.

K. "Trigger Data" means Personal Data which if subject to a security breach as defined by Applicable Data Protection Laws would trigger an obligation to provide a security breach notification to affected individuals and/or any government authority.

L. "Sub-processor" means an entity that Processes Personal Data at the request of, and subject to a written agreement with, Seller.

II. Seller's Processing Of Personal Data

A. Seller As Data Processor: Seller acknowledges that with respect to the Processing of Personal Data for purposes of performing the Services, Seller is the Data Processor, and Buyer is a Data Controller.

B. Permitted Processing Of Personal Data By Seller: Seller agrees to Process Personal Data solely (1) pursuant to Buyer's lawful instructions as reflected in the Terms and Conditions, (2) as necessary to perform the Services under the Terms and Conditions; and (3) in accordance with **Annex A**, which describes, among other things, the nature and purpose of the Processing, the type of Personal Data, Processed and the categories of Data Subjects.

C. Duration of Processing. Seller is permitted to Process Personal Data only for the duration of the term of the Terms and Conditions. Upon termination of the Terms and Conditions, Seller agrees to return or destroy, as provided in Section VII, below, all Personal Data Processed on Buyer's behalf in Seller's possession, except where local law requires Seller to retain categories of Personal Data in which case this Addendum shall survive termination, and Seller shall comply with this Addendum's terms for as long as the Personal Data remains in Seller's possession.

D. Compliance With Applicable Data Protection Laws. Seller may Process Personal Data only in accordance with Applicable Data Protection Laws. Seller will provide all assistance reasonably required by Buyer to enable Buyer to take reasonable and

appropriate steps to ensure that Seller effectively Processes Personal Data in a manner consistent with Buyer's obligations under Applicable Data Protection Laws. Seller will immediately notify Buyer if Seller becomes aware that Seller's compliance with any term or condition of this Addendum has violated, violates, or will violate Seller's or Buyer's obligations under Applicable Data Protection Laws. Seller will cooperate with Buyer as reasonably necessary to prevent or mitigate any Processing of Personal Data in violation of Applicable Data Protection Laws.

E. Disclosures Of Personal Data. Seller will maintain the confidentiality of all Personal Data Processed on behalf of Buyer. Seller may disclose Personal Data to a third party only (1) where the disclosure is Required By Law, (2) with the prior written consent of Buyer, (3) to a Data Subject, at Buyer's request, in response to an access request under Applicable Data Protection Laws, and (4) to a Sub-processor in compliance with Section VI, below. Before disclosing Personal Data as Required By Law, Seller will promptly notify Buyer in writing of such required disclosure and will provide Buyer a reasonable opportunity to object to the request before Seller produces any Personal Data in response.

III. Seller's Personnel With Access To Sensitive Personal Information

A. Confidentiality Agreement For Seller's Personnel: Seller warrants that it has required its personnel authorized to access Personal Data to execute an appropriate confidentiality agreement or otherwise to undertake to safeguard the confidentiality of any Personal Data Processed by Seller on Buyer's behalf.

B. Training For Seller's Personnel Seller shall ensure that its personnel engaged in Processing Personal Data have received appropriate training on their confidentiality obligations.

IV. Seller's Safeguards For Personal Data

A. Physical, Technical And Organizational Safeguards. Seller shall maintain a comprehensive written information security program that includes reasonable and appropriate measures — including technical, physical, and organizational safeguards taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons — to protect against reasonably foreseeable risks to the security, availability, confidentiality, integrity and resilience of Personal Data, which risks could result in the unauthorized disclosure, use, alteration, destruction or other compromise of the Personal Data, or the unavailability of Personal Data. Seller represents and warrants that such program complies with Applicable Data Protection Laws concerning the protection of Personal Data and, at a minimum, includes the organizational, physical, and technical safeguards listed in **Annex B**.

B. Validation Of Safeguards: Seller will provide Buyer with third-party validation attestations (SSAE 16, SOC Type 2, ISO 27002, TISAX, PCI ROC, or any similar report) for itself within thirty (30) days of the report's issuance. Any exceptions noted on the audit report will be promptly addressed with the development and implementation of a corrective action plan created by Seller, which shall be provided to and approved by Buyer. Buyer will treat any information received from Seller pursuant to this provision as confidential information.

C. Security Incident Response Plan. Seller will maintain (and, if necessary, develop and implement) a written response plan to ensure that any Security Incident will be promptly Discovered and promptly reported to Buyer.

D. Reporting Security Incidents. Seller will report to Buyer any Security Incident Discovered by Seller, regardless of whether the Security Incident results from the actions of Seller or its Sub-processors. Seller will make such report orally to Buyer within 48 hours of Seller's becoming aware of the Security Incident followed by a report in writing (e-mail is acceptable) within 24 hours of the initial oral report. The written report shall include, at a minimum subject to the availability of necessary information, the following: (1) a description of the Security Incident; (2) the date the Security Incident occurred; (3) the date the Security Incident was Discovered; (4) the affected categories of Personal Data for each affected Data Subject; (5) the approximate number of Data Subjects affected and the approximate number of records containing Personal Data; (6) an identification of any law enforcement agency or government authority that has been contacted about the Security Incident and contact information for the relevant official; (7) a description of the steps that have been, or will be, taken to mitigate the Security Incident; (8) a description of the steps that have been, or will be, taken to prevent a recurrence; (9) contact information for the person at Seller principally responsible for responding to the Security Incident; and (10) any other information that Buyer is required under Applicable Data Protection Law to provide in a notification to Data Subjects or to any government authority.

Seller will update the written report periodically as material, new information becomes available, including non-privileged forensics and root cause analysis. All reports required by this provision shall be made to cybersecurity@harman.com and privacy@harman.com. Seller acknowledges that its determination that a particular set of circumstances constitutes a security breach as defined by Applicable Data Protection Laws shall not be binding on Buyer.

E. Mitigation Of Damages By Seller And Cooperation in Investigation. Seller agrees to take, at its own expense, measures reasonably necessary to mitigate any harmful effect of a Security Incident. Seller agrees to cooperate, at its own expense, with Buyer in its investigation of any Security Incident. Seller will promptly reimburse Buyer for all imputed and out-of-pocket costs reasonably incurred by Buyer in connection with the Security Incident, including, but not limited to, costs related to Buyer's provision of notices to affected Data Subjects and to any services offered to affected Data Subjects.

F. Notifications Related To A Personal Data Breach. Seller acknowledges that Buyer shall determine (i) whether and when to notify any government authority and which government authority to notify; (ii) whether Buyer will provide notice to Data Subjects with respect to any Security Incident; (iii) the content of any such notice(s); (iv) the timing for, and method of, delivery of any such notice(s); and (v) the products or services, if any, to be offered to affected Data Subjects. At its election, Buyer may delegate to Seller any of Buyer's responsibilities under Applicable Data Protection Laws with respect to any Security Incident involving Personal Data in the possession, custody or control of Seller or its Sub-processors, and Seller accepts such delegation. In the event of such a delegation, Seller will send a notice to a government authority or affected Data Subjects on Buyer's behalf only after providing Buyer a reasonable

opportunity to review such notice(s) and only with Buyer's prior approval of such notice(s).

V. Seller's Assistance With Audits And Requests From Data Subjects

A. Availability Of Records Of Processing Activities: Seller shall keep, or cause to be kept, accurate records relating to its Processing of Personal Data in connection with the Services. Upon reasonable request by Buyer, Seller shall promptly make available to Buyer all information, including the records of its Processing activities and relevant policies and procedures, necessary to demonstrate Seller's compliance, in its performance of the Services, with this Addendum and Applicable Data Protection Laws.

B. Audits Of Seller's Processing Activities. Seller will permit Buyer, directly or through a third party, to conduct site audits of the information technology and information security controls for facilities used to Process Personal Data on behalf of Buyer so that Buyer can ensure that Seller provides the appropriate level of security for the Personal Data and Processes Personal Data in compliance with this Addendum and Applicable Data Protection Laws. Buyer and any third party that conducts an audit on Buyer's behalf will treat any information created or received during the course of any audit conducted pursuant to this provision as confidential information.

C. Requests For Impact Assessment Information. Seller shall promptly provide the information reasonably requested by Buyer to assist Buyer in conducting a data protection impact assessment when such assessment is required by Applicable Data Protection Laws.

D. Requests From Data Subjects. Seller shall provide Buyer with assistance reasonably necessary to allow Buyer to comply with its obligations to respond to any request by a Data Subject to exercise any right conferred on the Data Subject by Applicable Data Protection Laws. Seller will comply with the request within fifteen (15) business days of receiving the request from Buyer. Within five (5) business days or receiving a request directly from a Data Subject to exercise any right under Applicable Data Protection Laws, Seller will provide the Buyer with a copy of the request and await Buyer's instructions on how to respond. Seller will promptly inform Buyer if complying with a request from Buyer would adversely affect the rights and freedoms of others.

E. Inquiries From Government Authorities: Upon Buyer's reasonable request, Seller will provide assistance as may be reasonably necessary to enable Buyer to respond to, comply with, or otherwise resolve any request, question or complaint received from any government authority, including government authorities responsible for enforcing Applicable Data Protection Laws, relating in any way to the Processing of Personal Data.

VI. Seller's Sub-processors

A. Consent To Processing By Sub-Processors. Buyer consents to Seller's disclosure of Personal Data to the Sub-processors identified in Annex C. Seller shall provide Buyer with no less than thirty (30) days' notice before disclosing Personal Data to a Sub-processor not listed in Annex C. In the event, Buyer does not object to Seller's disclosure of Personal Data to any additional Sub-processor, Seller shall remain

responsible for, and liable to Buyer for, the acts and omissions of such Sub-processor with regard to Personal Data Processed by the Sub-processor on Buyer's behalf as if they were Seller's own acts and omissions. In addition, Buyer will revise Annex C to reflect the additional Sub-processors without further amendment of this Addendum. If Buyer objects to the new Sub-processor and the Parties cannot reasonably resolve the objection, Buyer may terminate the Terms and Conditions and this Addendum.

B. Sub-processors' Data Protection Obligations: Seller shall obtain reasonable assurances, in writing, from any Sub-processor to whom Seller discloses Personal Data. Such assurances by the Sub-processor will include at least the following: that the Sub-processor will (1) comply with the same restrictions and conditions on Processing Personal Data that this Addendum imposes on Seller; (2) implement reasonable and appropriate physical, technical and organizational safeguards to protect Personal Data in compliance with Applicable Data Protection Laws, and (3) notify Seller promptly after Discovering any Security Incident. If Schedule 1, 2, 3 or 4 in Section IX, below, is applicable, Seller shall ensure that it executes with Sub-processor any onward transfer agreement required by the applicable schedule.

VII. Seller's Obligations Upon Termination Of The Terms and Conditions.

A. Return Or Destruction Of Personal Data. Within fifteen (15) business days of the termination of the Terms and Conditions, Seller, at Buyer's election, shall return, destroy, or transfer to a third party designated by an authorized Buyer representative in writing, all Personal Data. If Buyer directs Seller to destroy the Personal Data, Seller shall do so in a manner reasonably intended to ensure that recovery of the Personal Data would be impracticable. Within ten (10) business days of the date of destruction, Seller will provide Buyer with a written certification, signed by an authorized representative, representing that the Personal Data has been permanently and securely destroyed and describing the method of destruction.

B. Seller's Retention Of Personal Data. If, at the termination of the Terms and Conditions, Seller delivers to Buyer written notice explaining the reasons that applicable law requires Seller to retain the Personal Data, then Buyer may excuse Seller from complying, in whole or in part, with Section VII.A, above. If Buyer excuses compliance with Section VII.A, in whole or in part, Seller agrees that, with respect to the Personal Data for which compliance with Section VII.A has been excused, Seller shall (1) deliver to Buyer, within fifteen (15) business days of the termination of the Terms and Conditions, a duplicate of all Personal Data retained by Seller; and (2) extend the protections of this Addendum to the retained Personal Data and limit further Processing of the retained Personal Data to those purposes for which applicable law requires retention, for as long as Seller maintains the Personal Data.

C. Survival. Seller's obligations and duties under this Addendum with respect to Personal Data shall survive the termination of the Terms and Conditions and of this Addendum and shall continue for as long as the Personal Data remains in the possession of Seller or of its Sub-processors.

VIII. Insurance And Indemnification

A. Seller's Insurance. Seller shall maintain cyber liability insurance with a limit of five million dollars ($5,000,000) per claim and in the aggregate per calendar year, including

coverage for costs arising from or relating to a Security Incident involving Trigger Data in the possession, custody or control of Seller or its Sub-processors.

B. Indemnification. Seller shall defend and indemnify Buyer, its parent and subsidiary corporations, officers, directors, employees and agents for any and all claims, inquiries, investigations, costs, reasonable attorneys' fees, monetary penalties, and damages incurred by Buyer and/or its parent or subsidiary corporations, officers, directors, employees and agents resulting from (1) any Processing of Personal Data in violation of this Agreement, (2) any Security Incident involving Trigger Data Processed on behalf of Buyer in the possession, custody or control of Seller or its Sub-processors, and (3) any other breach of the and this Agreement by Seller.

C. No Limitation Of Liability: There shall be no limitation of Seller's liability for (a) any breach by Seller of this Agreement, and (b) Seller's indemnification obligations under this Agreement.

IX. Jurisdiction-Specific Terms

A. The Parties acknowledge that Applicable Data Protection Laws in certain jurisdictions require the Parties to provide additional protections for Personal Data through written contract terms. Such jurisdiction-specific terms are contained in the following schedules and are incorporated by reference into this Addendum. The schedules are binding on the Parties as follows:

1) Schedule 1 (EEA): Schedule 1 applies when (a) Buyer is (i) located in the European Economic Area ("EEA"), or (ii) contracting on behalf of any member of its corporate group located in the EEA; and (b) Seller is located in a country outside the EEA and not subject to an Adequacy Determination. Schedule 1 is available at https://www.harman.com/supply-chain.

2) Schedule 2 (Switzerland): Schedule 2 applies when (a) Buyer is (i) located in Switzerland, or (ii) contracting on behalf of any member of its corporate group located in Switzerland; and (b) Seller is located in a country outside Switzerland and not subject to an Adequacy Determination. Schedule 2 is available at https://www.harman.com/supply-chain.

3) Schedule 3 (UK): Schedule 3 applies when (1) Buyer is (i) located in the United Kingdom ("UK"), or (ii) contracting on behalf of a member of its corporate group located in the UK; and (2) Seller is located in a country other than the UK and not subject to an Adequacy Determination. Schedule 3 is available at https://www.harman.com/supply-chain.

4) Schedule 4 (California, USA): Schedule 4 applies when Buyer, or a member of its corporate group and the Personal Data Processed by Seller are subject to the California Privacy Rights Act ("CPRA"). Schedule 4 is available at https://www.harman.com/supply-chain.

B. The Parties may add schedules to this Addendum, without the need for an amendment, as may be required to comply with changes to Applicable Data Protection

Laws to require the Parties to provide additional protections for Personal Data through a Data Transfer Agreement ("DTA").

C. In the event of any conflict between the terms of this Addendum and the terms of a DTA in any schedule, the terms of the DTA shall control.

X. Miscellaneous Terms

A. No Third-Party Beneficiaries. No third party shall be considered a third-party beneficiary under this Addendum, nor shall any third party have any rights as a result of this Addendum.

B. Construction. In the event of any inconsistency between this Addendum and the Terms and Conditions with respect to any matter falling within the scope of this Addendum, this Addendum shall control.

C. Modification. The Parties agree to amend this Addendum from time to time as may be necessary to permit Buyer to remain in compliance with Applicable Data Protection Laws.

Information Applicable To Data Processing Engagements Subject To Schedules 1, 2, or 3

1. The Parties To The Data Transfer Agreement:

    a. Schedule 1 (EEA):
        i. Data Exporter: Each member of the Harman corproate group that (a) falls within the definition of Buyer, and (b) is located in an EEA Member State.
        ii. Data Importer: Seller

    b. Schedule 2 (Switzerland): The competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.
        i. Data Exporter: Each member of the Harman corporate group that (a) falls within the definition of Buyer, and (b) is located in Switzerland
        ii. Data Importer: Seller

    c. Schedule 3 (UK): The competent supervisory authority is the UK Information Commissioner's Office.
        i. Data Exporter: Each member of the Harman corproate group that (a) falls within the definition of Buyer, and (b) is located in the UK.
        ii. Data Importer: Seller

2. Competent Supervisory Authoirty:

    a. Schedule 1 (EEA): The competent supervisory authority is the supervisory authority of the EEA Member State where the Data Exporter is established.

    b. Schedule 2 (Switzerland): The competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

    c. Schedule 3 (UK): The competent supervisory authority is the UK Information Commissioner's Office.