DATA PROCESSING ADDENDUM

This Data Processing Addendum, including the applicable schedules (collectively, the "Addendum"), supplements and is incorporated by reference into, the agreement entered between Harman International Industries, Incorporated, or one of its affiliated companies ("HARMAN") and [insert Seller legal entity name] ("Seller", and together with HARMAN, the "Parties", and each a "Party") regarding the provision of Seller's services (the "Agreement"). This Addendum shall become effective as of the effective date of the Agreement.

RECITALS

WHEREAS, in connection with the Agreement, Seller will receive Personal Data concerning HARMAN's prospective, current, and/or former employees and/or other Data Subjects;

WHEREAS, before disclosing Personal Data to Seller, HARMAN requires written assurances from Seller that Seller will Process Personal Data in accordance with all Applicable Data Protection Laws and HARMAN's requirements;

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 Personal Data.

C. "Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data and includes a "Business" or equivalent terms under Applicable Data Protection Laws.

D. "Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller and includes a "Service Provider" or equivalent terms under Applicable Data Protection Laws.

E. "Data Subject" means the natural person to whom the Personal Data pertains and includes a "Consumer" or other equivalent terms under Applicable Data Protection Laws.

F. "Data Subject Request" means a request by a Data Subject to exercise rights related to their Personal Data including to receive information about their Personal Data, obtain access to, modification of, or erasure of their Personal Data, to limit, opt out of, or otherwise object to the Processing of their Personal Data, and any other applicable rights conferred to Data Subjects under Applicable Data Protection Laws.

G. "Personal Data" means any information received by Seller from, or created or received by Seller on behalf of, HARMAN, 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. Personal Data includes "Personal Information" or other equivalent terms under Applicable Data Protection Laws.

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 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. "Security Incident" means the loss, or unauthorized access to, or use, disclosure, acquisition, modification, or destruction, of Personal Data, and includes "Personal Data Breach" or other equivalent terms under Applicable Data Protection Laws.

J. "Share" "Shared," or "Sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between HARMAN and Seller or Seller and a third party for cross-context behavioral advertising for the benefit of a Business in which no money is exchanged and also includes "Targeted Advertising" as defined under the California Privacy Rights Act (CPRA) or equivalent terms under Applicable Data Protection Laws.

II. Seller's Processing Of Personal Data

A. The Parties as Controllers: The Parties acknowledge that with respect to the Processing of Personal Data under this Agreement Seller and HARMAN are each independent, as applicable, Controllers.

B. Permitted Processing Of Personal Data By Seller: Seller agrees to Process Personal Data solely (1) 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 and (2) to the extent that Seller has a lawful basis for Processing the Personal Data; . Seller shall not sell, as that term is used in Applicable Data Protection Laws, any Personal Data. If HARMAN's disclosure of Personal Data to Seller or Seller's Processing of Personal Data under this Addendum constitute Sharing, Schedule A will apply.

C. Duration of Processing. Seller shall only Process Personal Data for the processing purposes permitted under Annex A for duration of the Agreement. This Addendum shall survive termination, and Seller shall comply with this Addendum for as long as Seller continues to Process the Personal Data or it otherwise remains in Seller's possession.

D. Compliance With Applicable Data Protection Laws. Both Parties shall Process Personal Data in accordance with the Applicable Data Protection Laws that apply to the Parties and in the jurisdiction in which the Personal Data is collected, in respect of the

performance of their respective obligations under the Addendum and the Agreement. Both Parties shall provide assistance reasonably required for each Party to comply with its obligations under Applicable Data Protection Laws.

E. Disclosures Of Personal Data. Seller will maintain the confidentiality of all Personal Data as set forth in this Addendum. Seller may disclose Personal Data to a third party only (1) where the disclosure is required by statute, regulation, court order, or legal process, (2) to a Processor in compliance with Applicable Data Protection Laws. If Seller is required to disclose Personal Data pursuant to Section II.E(1), Seller will promptly notify HARMAN in writing of such required disclosure and, to the extent permissible by law, provide HARMAN a reasonable opportunity to object to the request before Seller discloses any Personal Data in response to the request. Before Seller discloses Personal Data pursuant to Section II.E(2), Seller shall ensure that such third party is subject to contractual obligations as restrictive as those contained in this Addendum and as required by Applicable Data Protection Laws.

F. Confidentiality Agreement For Seller's Personnel: Seller warrants that any of its personnel who access or otherwise Process Personal Data are bound by confidentiality obligations as restrictive as those contained in this Addendum and as required by Applicable Data Protection Laws.

III. Seller's Safeguards For Personal Data

A. Physical, Technical And Organizational Safeguards. Seller shall implement appropriate technical, physical, and organizational safeguards to protect Personal Data 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 to the rights and freedoms of Data Subjects.

B. Reporting Security Incidents. Seller will provide notice without undue delay in the event Seller experiences a Security Incident, including reasonable assistance to HARMAN in satisfying HARMAN's Personal Data breach notification obligations, if any, under Applicable Data Protection Law. All notice required by this provision shall be made to cybersecurity@harman.com and privacy@harman.com.

IV. Cooperation Between the Parties

A. The Parties will provide reasonable assistance and cooperate with each other to assist in each Party's compliance with Applicable Data Protection Laws as relates to the Personal Data Processed pursuant to the Agreement.

B. Data Subject Requests. Each Party will respond directly to Data Subject Requests that it receives related to such Party's Processing of Personal Data. At the request of a Party who has received a Data Subject Request, the other Party will provide assistance reasonably necessary to allow the receiving party to comply with its obligations to respond to any Data Subject Request under Applicable Data Protection Laws.

C. Inquiries From Government Authorities: Each Party will provide the other Party reasonable cooperation 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 to Processing Personal Data under the Agreement. Each Party will promptly notify the other

Party if it receives such a complaint or inquiry.

V. 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.

B. Indemnification. Seller shall defend and indemnify HARMAN, 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 HARMAN and/or its parent or subsidiary corporations, officers, directors, employees and agents resulting from (1) any Processing of Personal Data by Seller in violation of this Agreement, (2) any Security Incident to the extent to which Seller's is found liable by a court of competent jurisdiction for the Security Incident as a result of Seller's action or inaction, 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 Addendum, and (b) Seller's indemnification obligations under this Addendum.

VI. 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 5 (EEA): Schedule 5 applies when (a) HARMAN 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 5 is available at https://www.harman.com/supply-chain.

2) Schedule 6 (Switzerland): Schedule 6 applies when (a) HARMAN 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 6 is available at https://www.harman.com/supply-chain.

3) Schedule 7 (UK): Schedule 7 applies when (1) HARMAN 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 7 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.

VII. 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 HARMAN to remain in compliance with Applicable Data Protection Laws.

Harman Int'l Industries	**Counterparty**
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____
Contact Person:_____	Contact Person:_____
Contact Title:_____	Contact Title:_____
Contact Email:_____	Contact Email:_____

Schedule A
Requirements when Sharing Personal Data

HARMAN is disclosing Personal Data to Seller only for the limited and specific purposes identified in Annex A to the Data Processing Addendum, Section C.1. Seller shall (i) Process Personal Data only for such limited and specific purposes, (ii) provide the same level of privacy protection to all Personal Data as is required by Applicable Data Protection Laws that apply to Sharing Personal Data, (iii) comply with all obligations under Applicable Data Protection Laws that apply to Sharing Personal Data, and (iv) notify HARMAN if it makes a determination that it can no longer meet such obligations. HARMAN may take reasonable and appropriate steps to help ensure that Seller uses Personal Data consistent with the HARMAN's obligations under Applicable Data Protection Laws that relate to Sharing Personal Data and to stop and remediate unauthorized use of Personal Data.

ANNEX A TO DATA PROCESSING ADDENDUM

(Details of the processing and, if, applicable, description of data transfers)

A. **Information Applicable To All Data Processing Engagements**

1. Nature Of Processing By Seller:

[INSERT]

2. Purposes Of Processing By Seller:

[INSERT]

3. Categories of Data Subjects Whose Personal Data Is Processed By Seller:

[INSERT]

4. Categories Of Personal Data Processed By Seller:

[INSERT]

5. Categories Of Sensitive Personal Data Processed By Seller:

[INSERT]

[**Note:** "Sensitive Personal Data" means (a) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (b) Personal Data concerning health, sex life, or sexual orientation; (c) genetic data, (d) biometric data when Processed for the purpose of uniquely identifying a natural person; (e) criminal history information; (f) government-issued identification number; (g) credit or debit card number; (h) financial account number in combination with any required security code, access code, or password that would permit access to a Data Subject's account; (j) health insurance information; and (k) i. a username or email address in combination with a password or security question and answer that would permit access to an online account.]

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

1. The Parties To The Data Transfer Agreement:
    a. Schedule 5 (EEA):
        i. Data Exporter: Each member of the HARMAN corporate group that (a) falls within the definition of HARMAN, and (b) is located in an EEA Member State.
        ii. Data Importer: Seller

    b. Schedule 6 (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 HARMAN, and (b) is located in Switzerland
        ii. Data Importer: Seller

    c. Schedule 7 (UK): The competent supervisory authority is the UK Information Commissioner's Office.
        i. Data Exporter: Each member of the HARMAN corporate group that (a) falls within the definition of HARMAN, and (b) is located in the UK.
        ii. Data Importer: Seller
        iii. Data Importer main address: _____
        iv. Official Registration Number: _____

    d. Contact Details:
        i. Data Exporter: [INSERT HARMAN CONTACT NAME, JOB TITLE, AND EMAIL ADDRESS]
    e. Data Importer: [INSERT CONTACT NAME, JOB TITLE, AND EMAIL ADDRESS]

2. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). [INSERT]

3. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period. [INSERT]

4. Competent Supervisory Authority:
    a. Schedule 5 (EEA): The competent supervisory authority is the supervisory authority of the EEA Member State where the Data Exporter is established or the supervisory authority of the EEA Member State in which the Data Exporter's Data Protection Representative is established.
    b. Schedule 6 (Switzerland): The competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.
    c. Schedule 7 (UK): The competent supervisory authority is the UK Information Commissioner's Office.

ANNEX C TO DATA PROCESSING ADDENDUM

Description of the technical and organizational 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.

I. ORGANIZATIONAL MEASURES

A. Information Security Governance

Data importer has established a personnel structure for information security governance, including but not limited to, a designated employee with overall responsibility for information security government (e.g., a chief information security officer) and other personnel with assigned roles and responsibilities for information security. Roles and responsibilities have been formally defined for all members of the information security team and have been documented.

B. Administrative Access Controls

1. Access Authorization and Workforce Clearance: An employee or contractor will be authorized to access personal data ("Authorized Users") only if the individual is deemed trustworthy based upon prior service to the data importer or the successful completion of a background check where permitted by applicable law. Data importer permits Authorized Users to access personal data only on a need-to-know basis and only as necessary to perform assigned job responsibilities.

2. Confidentiality Agreement: Before establishing access for an Authorized User, data importer requires that the Authorized User execute a confidentiality agreement that applies to the personal data or otherwise acknowledges an obligation of confidentiality.

3. Access Establishment: Data importer separates functions between those authorized to assign access rights and those authorized to establish access to data importer's information systems.

4. Review Of Access Rights: On at least a quarterly basis and when an Authorized User changes positions, data importer reviews and, if necessary, revises or terminated the Authorized User's rights of access to workstations, programs and processes to limit the Authorized User's access to personal data to the minimum necessary to perform assigned job functions. Data importer will delete any personal data stored on the Authorized User's computer that no longer is needed by the Authorized User in his or her new position.

5. Denial Of Access To Terminated Authorized Users: Upon termination of any Authorized User's relationship with data importer, data importer promptly does the following: (a0 terminate the Authorized User's rights to access personal data and obtain the return of any devices (such as tokens or key cards) used to obtain access to personal data; (b) obtain the return of all keys, key cards, and other devices that permit access to physical locations containing personal data in paper form; (c) ensure that the terminated Authorized User does not have unescorted access to areas containing personal data in paper form; (d) ensure that all personal data is removed from any computer equipment used by the terminated Authorized User before re-issuing that equipment to another Authorized User.

C. Training

Data importer provides (a) initial training to relevant personnel on how to implement and comply with its information security program, including identifying and reporting a personal data breach, and (b) periodic refresher training and security awareness reminders. Data importer permits newly hired Authorized Users to access personal data only after completion of the initial data security training.

D. Security Incident Response

Data importer has created a security incident response team (SIRT) with assigned roles and responsibilities. Data importer has implemented procedures for identifying security incidents, including personal data breaches, and a plan for responding to security incidents. Data importer periodically tests the security incident response plan. Data importer has established a mechanism for employees to report security incidents, including suspected and actual personal data breaches. Data importer requires all employees to immediately report the loss, theft, or otherwise of any equipment on which personal data is stored.

II. TECHNICAL MEASURES

A. Evaluation And Monitoring

1. Risk Assessment: Data importer has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of personal data. Data importer has implemented t policies and procedures to reduce risks and vulnerabilities to personal data to a reasonable and appropriate level. These policies and procedures are designed to protect the confidentiality, integrity and availability of personal data and to prevent accidental or unauthorized use, disclosure, alteration, loss or destruction.

2. Evaluation Of Security Policies And Procedures: Data importer periodically reviews and, if necessary, updates the policies and procedures described above, as necessary in response to environmental or operational changes affecting the security of personal data.

B. System Activity Review

1. Establishment Of Monitoring Procedures: Data importer has (a) enabled logging on computer systems that store personal data; (b) implemented a process for the review of exception reports and/or logs, and (c) developed and documented procedures for the retention of monitoring data.

2. Monitoring Of System Activity: Data importer periodically reviews information system activity records — including audit logs, access reports, privileged operations, error logs on servers, and security incident tracking reports, and changes to systems security — to ensure that implemented security controls are effective and that personal data has not been potentially compromised. Monitoring includes (a) reviewing changes affecting systems handling authentication, authorization, and auditing; (b) reviewing privileged access to production systems processing personal data; and (c) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

3. Compliance Review And Third-Party Audits: Data importer periodically reviews compliance with security policies and procedures. Data importer engages a third party, at least annually, to perform an independent audit which includes an assessment of data importer's information security program. Data importer will make the third-party audit report available to data exporter upon request.

C. Protections Against Malicious Actors

1. Network Security: Data importer maintains an up-to-date firewall and intrusion detection software. Data importer engages in security patch management to ensure that security patches are installed as soon as is reasonably practicable.

2. Anti-Malware Protection: Data importer ensures that protections against malicious software (e.g., anti-virus protection, spyware detection software, etc.) are installed before computers and other devices are connected to any of data importer's networked systems. The software is kept current.

D. Technical Access Controls

1. Unique User ID/Secure Passwords: All Authorized Users will be assigned a unique user ID and will be required to create a strong/complex password, or to use a biometric identifier, to access data importer's network. Systems requiring entry of a password suppress, mask or otherwise obscure the password so that it cannot be viewed by an unauthorized person. All passwords are encrypted while in storage. Authorized Users are required to change passwords on a regular basis. Authorized Users are prohibited form sharing passwords with any other person.

2. Access Restrictions: Data importer has implemented technical controls so that each Authorized User will be able to gain access only to those categories of personal data to which access is necessary to perform assigned job responsibilities.

3. Encryption: Data importer encrypts personal data in transit, using Transport Layer Security (TLS) encryption. Data importer encrypts personal data at rest using 256-bit AES encryption or stronger. Mobile devices and portable electronic storage media used to store personal data must be encrypted.

4. Remote Access: Data importer permits remote access to its networks only via a Virtual Private Network ("VPM") or a similar secure means

5. Secure Disposal: Data importer has established procedures for the secure and permanent destruction of personal data stored in paper and electronic form.

E. Contingency Planning

1. Back-Ups: Data importer backs up personal data on a regular schedule (e.g., at least every 24 hours). Back-ups are encrypted and stored in a location physically apart from the primary storage. Back-ups permit prompt restoration of personal data in the event of a disaster.

2. Business Continuity/Disaster Recovery: Data importer has developed and maintains a business continuity/disaster recovery plan to ensure that data importer can promptly resume service and restore data exporter's access to personal data in the event of a physical or technical incident occurrence (for example, fire, ransomware attack, vandalism, system failure, pandemic flu, and natural disaster).

F. Change and Configuration Management

Data importer maintains policies and procedures for managing changes to production systems, applications, and databases processing personal data and for documenting the changes.

III. PHYSICAL SAFEGUARDS

1. Data importer's facilities where personal data are physically secured against unauthorized access by, for example, keys, access cards, receptionists, and/or security guards. Data importer requires that all employees where a security badge at all time while on data importer's premises. Guests and service providers must register at the reception area and are prohibited from unescorted access to data importer's facility.

2. All servers and network equipment containing personal data are maintained in a location subject to controlled physical access. Only authorized employees may have unescorted access to secure areas where servers and network equipment are located. Video surveillance cameras monitor secured areas where servers and other network equipment are located.

3. Only authorized employees may have unescorted access to areas with computers and other electronic resources that permit access to personal data. Access is restricted by a proximity card or key, receptionist, or some similar method. Physical access rights must be promptly terminated when an employee no longer needs physical access to areas containing electronic resources that permit access to personal data

4. Data exporter requires authorized employees to ensure that all electronic resources permitting access to personal data, including peripherals (computers, monitors, laptop computers, printers, digital cameras, projectors, etc.) that are assigned to, or regularly used by, them are maintained and used in a manner consistent with their function and such that the possibility of damage and/or loss is minimized.

5. Except for equipment designed to be portable, such as laptops, computer equipment used to access personal data should not be removed from data importer's premises without prior authorization.

IV. PERSONAL DATA MANAGEMENT

A. Data Minimization

Data importer has subjected its systems and applications used to process personal data to a review for compliance with privacy-by-design and privacy-default principles and has applied the results of that review to the design of its systems and applications that process personal data. Data importer's systems and applications have been designed to collect, use, disclose, and otherwise process the minimum personal data necessary to provide the services that are the subject of the Parties' underlying agreement. Data importer's systems and applications have been

programmed to automatically delete personal data in accordance with data exporter's data retention schedules or data retention instructions unless data importer is required by law to retain personal data for a longer period of time

B. Accountability

Data importer maintains a record of processing activities ("ROPA") that complies with GDPR, art. 30, with respect to its processing of personal data received form, or created or received on behalf of, data exporter. Data importer makes each relevant ROPA available to data exporter upon request.

C. Data Subject Rights

1. Correction/Update Of Personal Data: Data importer provides self-help options through its website to allow data subjects to correct and update their personal data and/or provides multiple methods (e.g., chat bot, webform, e-mail address) by which data subjects may submit requests for the correction and updating of their personal data.

2. Erasure: Data importer has established internal procedures and technical mechanisms to ensure that personal data can be permanently deleted from production systems and back-ups in response to a request from a data subject, if and to the extent required by GDPR, art. 17.

D. Data Portability:

Data importer has implemented procedures and systems that allow data importer to identify Personal Data provided by the data subject and to transfer that personal data, in a usable form, to a third party at the data subject's direction or to the data subject directly or by way of a storage medium.