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", and together with HARMAN, 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, before disclosing Personal Data to Seller, Buyer requires written assurances from Seller that Seller 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 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, 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. 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. "Sub-processor" means an entity that Processes Personal Data at the request of or on behalf or Seller and includes "Subcontractors" or other equivalent terms under Applicable Data Protection Laws.

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 a Data Processor, and Buyer is a Data Controller or Data Processor.

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 for and for the purposes of performing 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 unless otherwise provided herein. Upon termination of the Terms and Conditions, Seller shall return, destroy or transfer to a third party designated in writing by Buyer all Personal Data in Seller's possession, except where applicable law requires Seller to retain categories of Personal Data. Buyer reserves the right to elect whether Seller returns, destroys or transfers all Personal Data, and Seller shall satisfy any such request within thirty (30) days of receipt. If Buyer requests or Seller otherwise elects to destroy the Personal Data, Seller shall ensure that such destruction does not allow recovery of the Personal Data and shall certify in writing to Buyer when the Personal Data has been permanently and securely destroyed with a description of the method of destruction. If applicable law requires Seller to retain categories of Personal Data, Seller will notify Buyer in writing explaining the applicable reasons, Seller will limit further Processing of the retained Personal Data to only the purposes required by applicable law, 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. Seller shall Process Personal Data in accordance with Applicable Data Protection Laws. Seller will provide all assistance reasonably required by Buyer to comply with its 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 remediate 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 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) with the prior written consent or authorization of Buyer, and (3) to a Sub-processor in compliance with Section VI. Before disclosing Personal Data pursuant to this Section II.E(1), Seller will promptly notify Buyer in writing of such required disclosure and, to the extent permissible by law, provide Buyer a reasonable opportunity to object to the request before Seller discloses any Personal Data in response to the request.

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 required by Applicable Data Protection Laws.

G. Training For Seller's Personnel: Seller shall ensure that its personnel who Process Personal Data have received appropriate training regarding their confidentiality obligations.

III. 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 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 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. Seller represents and warrants that such safeguards comply with Applicable Data Protection Laws concerning the protection of Personal Data and, at a minimum, include the organizational, physical, and technical safeguards listed in **Annex C** or the equivalent thereof.

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 at Seller's expense . 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, regardless of whether the Security Incident results from the actions of Seller or its Sub-processors, without undue delay but no later than 72 hours of Seller's becoming aware of the Security Incident unless such report is restricted by law. Subject to the availability of information, Seller shall provide Buyer the following information: (1) a description of the Security Incident; (2) the date the Security Incident occurred; (3) the date Seller became aware of the Security Incident; (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 and contact information for the relevant official(s); (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 may reasonably request to allow Buyer to satisfy its obligations to notify Data Subjects or any government authority.

Seller will update Buyer 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 Seller's determination that a particular set of circumstances constitutes a Security Incident under 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 investigation of any Security Incident. To the extent Seller's actions or inaction caused a 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 Security Incident. Seller acknowledges that, unless otherwise required by Applicable Data Protection Laws, Buyer shall determine for any Security Incidents (i) whether and when notice will be provided to any government authority and which government authority to notify; (ii) whether and when notice will be provided to Data Subjects; (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).

IV. Seller's Assistance With Audits And Requests From Data Subjects and Regulatory Authorities

A. Information Demonstrating Compliance: Seller shall, upon Buyer's reasonable request, provide all reasonably necessary information to demonstrate Seller's compliance with Applicable Data Protection Laws.

B. Audits Of Seller's Processing Activities. Seller will permit and contribute to reasonable audits by Buyer, directly or through a third party, or arrange for an annual audit by a qualified independent auditor of the Seller's policies, and technical and organizational measures related to Seller's Processing of Personal Data to confirm whether 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. Any audits under this provision are subject to Buyer giving Seller reasonable prior notice of such audit and ensuring that any third-party auditor is not a competitor of Seller. Buyer and any third party auditor 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. Data Subject Requests. Seller shall provide Buyer with assistance reasonably necessary to allow Buyer to comply with its obligations to respond to any Data Subject Request under Applicable Data Protection Laws. Upon receipt of a Data Subject Request, Seller shall promptly but in any event no later than 10 days after receiving a Data Subject Request Seller shall notify Buyer and provide all reasonable assistance with responding to the request and Buyer will be responsible for responding to any such request. Seller shall not respond to any Data Subject Request unless instructed by Buyer in writing to do so.

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 Seller's Processing of Personal Data.

V. 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 B. Seller shall notify Buyer at least thirty (30) days before disclosing Personal Data to a Sub-processor not listed in Annex B, and Buyer will have the right to object. If Buyer does not object, Annex B will be deemed to have been amended to reflect the new Sub-processor. If Buyer objects to the new Sub-processor and the Parties cannot reasonably resolve the objection, Buyer may in whole or in part terminate the Terms and Conditions and this Addendum in respect to the aspects of the Services that are impacted by the use of any Sub-processor to which Buyer objects.

B. Sub-processors' Data Protection Obligations: Seller shall only engage Sub-processors pursuant to a written contract that satisfies Applicable Data Protection Laws and includes 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 becoming aware of any Security Incident. If Schedule 1, 2, 3 or 4 in Section VII, below, is applicable, Seller shall ensure that it executes with Sub- processor any onward transfer agreement required by the applicable schedule.

VI. 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.

v

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 by Seller in violation of this Addendum, (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 Addendum 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.

VII. 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.

VIII. 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.

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:_____

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 1 (EEA):
        i. Data Exporter: Each member of the HARMAN corporate 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 corporate group that (a) falls within the definition of Buyer, 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 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 1 (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 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.**Information Applicable To Data Processing Engagements Subject To Schedule 4**

1. The specific services for which Seller may Process Personal Information are as follows:

[insert brief description or reference a specific section of the service agreement]

2. Buyer is disclosing Personal Information to Seller only for the following specific Business Purposes (check all that apply):

☐ Performing services on behalf of Buyer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of Buyer;

☐ Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;

☐ Helping to ensure security and integrity to the extent the use of Buyer's Personal Information is reasonably necessary and proportionate for these purposes;

☐ Debugging to identify and repair errors that impair existing intended functionality;

☐ Short–term, transient use, including, but not limited to, non-personalized advertising shown as part of a Consumer's current interaction with Buyer, provided that Buyer's Personal Information is not disclosed to another third party and is not used to build a profile about the Consumer or otherwise alter the Consumer's experience outside the current interaction with Buyer;

☐ Providing advertising and marketing services, except for cross-context behavioral advertising, to Buyer provided that, for the purpose of advertising and marketing, Seller shall not combine the Personal Information of opted-out Consumers that Seller receives from, or on behalf of, Buyer with personal information that Seller receives from, or on behalf of, another person or persons or collects from its own interaction with Consumers;

☐ Undertaking internal research for technological development and demonstration;

☐ Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by Buyer, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by Buyer.

ANNEX B TO DATA PROCESSING ADDENDUM

Buyer agrees to Seller's use of the sub-processors identified on the list of sub-processors located on Seller's website at the following URL to Process Personal Data on the condition of a contractual agreement in accordance with this Addendum and Applicable Data Protection Laws: [**insert URL**]

If Seller does not post a list of its Sub-processors on its website, Buyer agrees to Seller's use of the following Sub-processors to Process Personal Data on the condition of a contractual agreement in accordance with this Addendum and Applicable Data Protection Laws:

Sub-processor's Name	**Subject Matter and Nature of Sub-processing Services**	**Description Of Sub-processing Services**

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.