AWS DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the AWS Customer Agreement available at http://aws.amazon.com/agreement, as updated from time to time between Customer and AWS, or other agreement between Customer and AWS governing Customer's use of the Services (the "**Agreement**"). This DPA is an agreement between you and the entity you represent ("**Customer**", "**you**" or "**your**") and Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together "**AWS**"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 17 of this DPA.

1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by AWS. In this context, AWS will act as processor to Customer, who can act either as controller or processor of Customer Data.

1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations under Applicable Data Protection Law, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if AWS becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.

1.3 Details of Data Processing.

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.

1.3.2 **Duration.** As between AWS and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 **Nature of the processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5 **Type of Customer Data.** Customer Data uploaded to the Services under Customer's AWS accounts.

1.3.6 **Categories of data subjects.** The data subjects could include Customer's customers, employees, suppliers and End Users.

1.4 **Compliance with Laws**. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Applicable Data Protection Law.

2. Customer Instructions. The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer's documented instructions regarding AWS's processing of Customer Data ("**Documented Instructions**"). AWS will process

Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between AWS and Customer, including agreement on any additional fees payable by Customer to AWS for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if AWS declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely AWS can form an opinion on whether Documented Instructions infringe Applicable Data Protection Law. If AWS forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3. Confidentiality of Customer Data. AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.

4. Confidentiality Obligations of AWS Personnel. AWS restricts its personnel from processing Customer Data without authorization by AWS as described in the Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Security of Data Processing

5.1 AWS has implemented and will maintain the technical and organizational measures for the AWS Network as described in the Security Standards and this Section. In particular, AWS has implemented and will maintain the following technical and organizational measures:

(a) security of the AWS Network as set out in Section 1.1 of the Security Standards;

(b) physical security of the facilities as set out in Section 1.2 of the Security Standards;

(c) measures to control access rights for authorized personnel to the AWS Network as set out in Section 1.3 of the Security Standards; and

(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by AWS as described in Section 2 of the Security Standards.

5.2 Customer can elect to implement technical and organizational measures to protect Customer Data. Such technical and organizational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third-party supplier:

(a) pseudonymization and encryption to ensure an appropriate level of security;

(b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;

measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

(c) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

6. Sub-processing.

6.1 **Authorized Sub-processors.** Customer provides general authorization to AWS's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The AWS website (currently posted at https://aws.amazon.com/compliance/sub-processors/) lists Sub-processors that are currently engaged by AWS. At least 30 days before AWS engages a Sub-processor, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or (iii) move the relevant Customer Data to another Region where AWS has not engaged the Sub-processor.

6.2 **Sub-processor Obligations.** Where AWS authorizes a Sub-processor as described in Section 6.1:

(i) AWS will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Data for any other purpose;

(ii) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this DPA, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this DPA; and

(iii) AWS will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause AWS to breach any of AWS's obligations under this DPA.

7. AWS Assistance with Data Subject Requests. Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which AWS will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under Applicable Data Protection Law. If a data subject makes a request to AWS, AWS will promptly forward such request to Customer once AWS has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, AWS to respond to any data subject who makes a request to AWS, to confirm that AWS has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and AWS forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. Optional Security Features. AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and

(d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

9. Security Incident Notification.

9.1 **Security Incident.** AWS will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

9.2 **AWS Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as AWS is able to disclose to Customer, taking into account the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

9.3 **Unsuccessful Security Incidents.** Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of AWS's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) AWS's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by AWS of any fault or liability of AWS with respect to the Security Incident.

9.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console and secure transmission at all times.

10. AWS Certifications and Audits.

10.1 **AWS ISO-Certification and SOC Reports.** In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

(i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and

(ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls

implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

10.2 **AWS Audits.** AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third-party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be AWS's Confidential Information.

10.3 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA.

10.4 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information AWS makes available under this Section 10.

11. Customer Audits. Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under Applicable Data Protection Law or the Standard Contractual Clauses, by instructing AWS to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement. If AWS declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.

12. Transfers of Personal Data.

12.1 **Regions.** Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "**Region**"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or valid and binding order of a governmental body.

12.2 **Application of Standard Contractual Clauses.** Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data subject to the GDPR that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").

12.2.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

12.2.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer's controllers because AWS has no direct relationship with Customer's controllers and therefore, Customer will fulfil AWS's obligations to Customer's controllers under the Processor-to-Processor Clauses.

12.3 **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.

13. **Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the "**Termination Date**").

14. **Return or Deletion of Customer Data**. At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.

15. **Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

16. **Entire Agreement; Conflict**. This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.

17. **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

"**API**" means an application program interface.

"**Applicable Data Protection Law**" means all laws and regulations applicable to and binding on the processing of Customer Data by a party, including, as applicable, the GDPR and the UK Data Protection Act 2018.

"**AWS Network**" means the servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS's control and are used to provide the Services.

"**Binding Corporate Rules**" has the meaning given to it in the GDPR.

"**controller**" has the meaning given to it in the GDPR.

"**Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf.

"**Customer Data**" means the "personal data" (as defined in Applicable Data Protection Law) that is uploaded to the Services under Customer's AWS accounts.

"**Documentation**" means the then-current documentation for the Services located at http://aws.amazon.com/documentation (and any successor locations designated by AWS).

"**EEA**" means the European Economic Area.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"**processor**" has the meaning given to it in the GDPR.

"Processor-to-Processor Clauses" means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf.

"Region" has the meaning given to it in Section 12.1 of this DPA.

"Security Incident" means a breach of AWS's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"**Security Standards**" means the security standards attached to this DPA as Annex 1.

"Service Controls" means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

"Standard Contractual Clauses" means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.

"Third Country" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1

Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1 Information Security Program. AWS will maintain an information security program designed to (a) enable Customer to secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the AWS Network, and (c) minimize physical and logical security risks to the AWS Network, including through regular risk assessment and testing. AWS will designate one or more employees to coordinate and be accountable for the information security program.

AWS's information security program will include the following measures:

1.1 Logical Security.

A. Access Controls. AWS will make the AWS Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. AWS will maintain access controls and policies to manage authorizations for access to the AWS Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain access controls designed to (i) restrict unauthorized access to data, and (ii) segregate each customer's data from other customers' data.

B. Restricted User Access. AWS will (i) provision and restrict user access to the AWS Network in accordance with least privilege principles based on personnel job functions, (ii) require review and approval prior to provisioning access to the AWS Network above least privileged principles, including administrator accounts; (iii) require at least quarterly review of AWS Network access privileges and, where necessary, revoke AWS Network access privileges in a timely manner, and (iv) require two-factor authentication for access to the AWS Network from remote locations.

C. Vulnerability Assessments. AWS will perform regular external vulnerability assessments and penetration testing of the AWS Network, and will investigate identified issues and track them to resolution in a timely manner.

D. Application Security. Before publicly launching new Services or significant new features of Services, AWS will perform application security reviews designed to identify, mitigate and remediate security risks.

E. Change Management. AWS will maintain controls designed to log, authorize, test, approve and document changes to existing AWS Network resources, and will document change details within its change management or deployment tools. AWS will test changes according to its change management standards prior to migration to production. AWS will maintain processes designed to detect unauthorized changes to the AWS Network and track identified issues to a resolution.

F. Data Integrity. AWS will maintain controls designed to provide data integrity during transmission, storage and processing within the AWS Network. AWS will provide Customer the ability to delete Customer Data from the AWS Network.

G. Business Continuity and Disaster Recovery. AWS will maintain a formal risk management program designed to support the continuity of its critical business functions ("**Business Continuity Program**"). The Business Continuity Program includes processes and procedures for identification of, response to, and recovery from, events that could prevent or materially impair AWS's provision of the Services (a

"**BCP Event**"). The Business Continuity Program includes a three-phased approach that AWS will follow to manage BCP Events:

(i) **Activation & Notification Phase.** As AWS identifies issues likely to result in a BCP Event, AWS will escalate, validate and investigate those issues. During this phase, AWS will analyze the root cause of the BCP Event.

(ii) **Recovery Phase.** AWS assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.

(iii) **Reconstitution Phase.** AWS leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services and AWS Network have been restored. Following such confirmation, AWS conducts a post-mortem analysis of the BCP Event.

H. Incident Management. AWS will maintain corrective action plans and incident response plans to respond to potential security threats to the AWS Network. AWS incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The AWS incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation. AWS will maintain an AWS Security Bulletin (as of the Effective Date, http://aws.amazon.com/security/security-bulletins/) which publishes and communicates security related information that may affect the Services and provides guidance to mitigate the risks identified.

I. Storage Media Decommissioning. AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.

1.2 Physical Security.

A. Access Controls. AWS will (i) implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the AWS Network, (ii) use appropriate control devices to restrict physical access to the AWS Network to only authorized personnel who have a legitimate business need for such access, (iii) monitor physical access to the AWS Network using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, (iv) log and regularly audit physical access to the AWS Network, and (v) perform periodic reviews to validate adherence with these standards.

B. Availability. AWS will (i) implement redundant systems for the AWS Network designed to minimize the effect of a malfunction on the AWS Network, (ii) design the AWS Network to anticipate and tolerate hardware failures, and (iii) implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

1.3 AWS Employees.

A. Employee Security Training. AWS will implement and maintain employee security training programs regarding AWS information security requirements. The security awareness training programs will be reviewed and updated at least annually.

B. Background Checks. Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation

that is reasonable and appropriate for that employee's position and level of access to the AWS Network.

2 Continued Evaluation. AWS will conduct periodic reviews of the information security program for the AWS Network. AWS will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.