UK G-Cloud 13 Framework Agreement

AWS EMEA SARL, UK Branch - Supplier Terms

May 2022

Submitted By:

Chris Hayman
Director, UK Public Sector aws-gcloud@amazon.com

Neil Hall
Snr. Business Manager, Contracts aws-gcloud@amazon.com

Table of Contents

1.0 INTRODUCTION

1.1 General

This document provides the Supplier Terms for this Amazon Web Services EMEA SARL, UK Branch service offering made available on the Digital Marketplace for the G-Cloud 13 Framework Agreement.

The order of precedence for these Supplier Terms is addressed in the G-Cloud 13 Framework Agreement at Section 8.3 titled “Order of precedence”. In the event of a conflict or ambiguity, the order of precedence detailed in the G-Cloud 13 Framework Agreement shall apply.

In order to minimize the potential for ambiguity between the Supplier Terms and the Framework Agreement, the following principles should be applied when interpreting the Supplier Terms:

- Rights for Supplier to modify or change the Services and pricing are subject to the Section 9.1 of the Framework Agreement.
- Service Fees and billing shall be conducted in accordance with the invoicing profile outlined in the Order Form and the pricing in the Digital Marketplace.
- Individual Services may have additional terms and conditions that are unique to that particular type of Service that will apply in addition to the terms in this document. These are available at http://aws.amazon.com/serviceterms.
- Notwithstanding anything to the contrary in the Supplier Terms, The governing law of the Supplier Terms is the laws of England and Wales

Should the Buyer choose to (i) purchase products or Services that are not offered on the Digital Marketplace, or (ii) consume Services outside of the Terms stated in the Order Form, such products and services are not subject to the terms of the Framework Agreement, Call-Off Contract or these Supplier Terms and instead are governed exclusively by the terms of the Amazon Web Services on-line click through Customer Agreement (https://aws.amazon.com/agreement/). Buyers acknowledge that Supplier is unable to and has no responsibility to monitor Buyer accounts or limiting Buyers to stay within the G-Cloud 13 Framework Agreement terms. This is solely a Buyer responsibility.

1.2 Definition alignment

Definitions set out in the Framework Agreement and Call-Off Contract shall have the same meaning in the Supplier Terms.

The definitions set out in these Supplier Terms detailed in the table below shall be interpreted as follows to align to the definitions in the Framework Agreement and Call-Off Contract:

Supplier Terms definition	**Interpretation**
Agreement	shall mean this Supplier Terms document
AWS, we, us, or **our**	shall mean the Supplier
AWS Confidential Information	shall include Suppliers Confidential Information
AWS Content	shall include Suppliers Background IPR
AWS Contracting Party	shall mean the Supplier (Amazon Web Services EMEA SARL, UK Branch)
AWS Marks	shall include Suppliers Know-How
Customer	shall mean the Buyer
Customer Data	shall include Buyer Personal Data uploaded to the Services under Buyers accounts.
Documentation	shall include the Suppliers Application
Effective Date	shall mean the Start Date of the Call-Off Contract, as identified on the Order Form.
End User	Shall include the Buyer and any individual or entity that access or uses the Services

GDPR	shall mean the General Data Protection Regulation (Regulation (EU) 2016/679)
Governing Laws Governing Courts	shall mean the law of England and Wales and the courts of England and Wales respectively.
Losses	shall include Loss
Security Incident	Shall include Data Loss Event
Service	shall have the meaning set out in Schedule 3 (Glossary and Interpretations) of the Framework Agreement)
Service Offerings	shall mean the Service Definitions that Supplier publishes on the Digital Marketplace, as may be updated from time to time in accordance with the Framework Agreement.
Term	shall mean the term of the Call-Off Contract as set out in the Order Form.
Termination Date	shall mean the End date detailed in a Call-Off Contract with an individual Buyer.
you or **your**	shall mean the Buyer
Your Content	Shall include Service Data

All other definitions described in these Supplier Terms shall have the meaning set out herein.

2.0 AWS CUSTOMER AGREEMENT

THE FOLLOWING AWS CUSTOMER AGREEMENT AND RELEVANT APPENDICES APPLY AND ARE INCORPORATED TO EACH CALL-OFF CONTRACT ISSUED UNDER THE G-CLOUD 13 FRAMEWORK AGREEMENT AS THE "SUPPLIER TERMS".

This AWS Customer Agreement (this "**Agreement**") contains the terms and conditions that govern your access to and use of the Service Offerings (as defined below) and is an agreement between the applicable AWS Contracting Party specified in Section 14 below (also referred to as "**AWS**," "**we**," "**us**," or "**our**") and you or the entity you represent ("**you**" or "**your**"). This Agreement takes effect when you click an "I Accept" button or check box presented with these terms or, if earlier, when you use any of the Service Offerings (the "**Effective Date**"). You represent to us that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into this Agreement for an entity, such as the company you work for, you represent to us that you have legal authority to bind that entity. Please see Section 14 for definitions of certain capitalized terms used in this Agreement.

1. Use of the Service Offerings.

1.1 Generally. You may access and use the Services in accordance with this Agreement. Service Level Agreements and Service Terms apply to certain Service Offerings. You will comply with the terms of this Agreement and all laws, rules and regulations applicable to your use of the Service Offerings.

1.2 Your Account. To access the Services, you must have an AWS account associated with a valid email address and a valid form of payment. Unless explicitly permitted by the Service Terms, you will only create one account per email address.

1.3 Third-Party Content. Third-Party Content may be used by you at your election. Third-Party Content is governed by this Agreement and, if applicable, separate terms and conditions accompanying such Third-Party Content, which terms and conditions may include separate fees and charges.

2. Changes.

2.1 To the Services. We may change or discontinue any of the Services from time to time. We will provide you at least 12 months' prior notice if we discontinue material functionality of a Service that you are using, or materially alter a customer-facing API that you are using in a backwards-incompatible fashion, except that this notice will not be required if the 12 month notice period (a) would pose a security or intellectual property issue to us or the Services, (b) is economically or technically burdensome, or (c) would cause us to violate legal requirements.

2.2 To the Service Level Agreements. We may change, discontinue or add Service Level Agreements from time to time in accordance with Section 12.

3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. You may specify the AWS regions in which Your Content will be stored. You consent to the storage of Your Content in, and transfer of Your Content into, the AWS regions you select. We will not access or use Your Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. We will not (a) disclose Your Content to any government or third party or (b) move Your Content from the AWS regions selected by you; except in each case as necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body, we will give you notice of any legal requirement or order referred to in this Section 3.2. We will only use your Account Information in accordance with the Privacy Notice, and you consent to such usage. The Privacy Notice does not apply to Your Content.

4. Your Responsibilities.

4.1 Your Accounts. Except to the extent caused by our breach of this Agreement, (a) you are responsible for all activities that occur under your account, regardless of whether the activities are authorized by you or undertaken by you, your employees or a third party (including your contractors, agents or End Users), and (b) we and our affiliates are not responsible for unauthorized access to your account.

4.2 Your Content. You will ensure that Your Content and your and End Users' use of Your Content or the Service Offerings will not violate any of the Policies or any applicable law. You are solely responsible for the development, content, operation, maintenance, and use of Your Content.

4.3 Your Security and Backup. You are responsible for properly configuring and using the Service Offerings and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

4.4 Log-In Credentials and Account Keys. AWS log-in credentials and private keys generated by the Services are for your internal use only and you will not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.
4.5 End Users. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Service Offerings. You are responsible for End Users' use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under this Agreement and that the terms of your agreement with each End User are consistent with

this Agreement. If you become aware of any violation of your obligations under this Agreement caused by an End User, you will immediately suspend access to Your Content and the Service Offerings by such End User. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide such support or services.

5. Fees and Payment.

5.1 Service Fees. We calculate and bill fees and charges monthly. We may bill you more frequently for fees accrued if we suspect that your account is fraudulent or at risk of non-payment. You will pay us the applicable fees and charges for use of the Service Offerings as described on the AWS Site using one of the payment methods we support. All amounts payable by you under this Agreement will be paid to us without setoff or counterclaim, and without any deduction or withholding. Fees and charges for any new Service or new feature of a Service will be effective when we post updated fees and charges on the AWS Site, unless we expressly state otherwise in a notice. We may increase or add new fees and charges for any existing Services you are using by giving you at least 30 days' prior notice. We may elect to charge you interest at the rate of 1.5% per month (or the highest rate permitted by law, if less) on all late payments.

5.2 Taxes. Each party will be responsible, as required under applicable law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on that party upon or with respect to the transactions and payments under this Agreement. All fees payable by you are exclusive of Indirect Taxes, except where applicable law requires otherwise. We may charge and you will pay applicable Indirect Taxes that we are legally obligated or authorized to collect from you. You will provide such information to us as reasonably required to determine whether we are obligated to collect Indirect Taxes from you. We will not collect, and you will not pay, any Indirect Tax for which you furnish us a properly completed exemption certificate or a direct payment permit certificate for which we may claim an available exemption from such Indirect Tax. All payments made by you to us under this Agreement will be made free and clear of any deduction or withholding, as may be required by law. If any such deduction or withholding (including but not limited to cross-border withholding taxes) is required on any payment, you will pay such additional amounts as are necessary so that the net amount received by us is equal to the amount then due and payable under this Agreement. We will provide you with such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under this Agreement.

6. Temporary Suspension.

6.1 Generally. We may suspend your or any End User's right to access or use any portion or all of the Service Offerings immediately upon notice to you if we determine:

(a) your or an End User's use of the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) could adversely impact our systems, the Service Offerings or the systems or Content of any other AWS customer, (iii) could subject us, our affiliates, or any third party to liability, or (iv) could be fraudulent;

(b) you are, or any End User is, in breach of this Agreement;
(c) you are in breach of your payment obligations under Section 5; or
(d) you have ceased to operate in the ordinary course, made an assignment for the benefit of creditors or similar disposition of your assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceeding.

6.2 Effect of Suspension. If we suspend your right to access or use any portion or all of the Service Offerings:

(a) you remain responsible for all fees and charges you incur during the period of suspension; and

(b) you will not be entitled to any service credits under the Service Level Agreements for any period of suspension.

7. Term; Termination.

7.1 Term. The term of this Agreement will commence on the Effective Date and will remain in effect until terminated under this Section 7. Any notice of termination of this Agreement by either party to the other must include a Termination Date that complies with the notice periods in Section 7.2.

7.2 Termination.

(a) Termination for Convenience. You may terminate this Agreement for any reason by providing us notice and closing your account for all Services for which we provide an account closing mechanism. We may terminate this Agreement for any reason by providing you at least 30 days' advance notice. (b) Termination for Cause.

(i) By Either Party. Either party may terminate this Agreement for cause if the other party is in material breach of this Agreement and the material breach remains uncured for a period of 30 days from receipt of notice by the other party. No later than the Termination Date, you will close your account. (ii) By Us. We may also terminate this Agreement immediately upon notice to you (A) for cause if we have the right to suspend under Section 6, (B) if our relationship with a third-party partner who provides software or other technology we use to provide the Service Offerings expires, terminates or requires us to change the way we provide the software or other technology as part of the Services, or (C) in order to comply with the law or requests of governmental entities.

7.3 Effect of Termination.

(a) Generally. Upon the Termination Date:

(i) except as provided in Section 7.3(b), all your rights under this Agreement immediately terminate;

(ii) you remain responsible for all fees and charges you have incurred through the Termination Date and are responsible for any fees and charges you incur during the post-termination period described in Section 7.3(b);

(iii) you will immediately return or, if instructed by us, destroy all AWS Content in your possession; and

(iv) Sections 4.1, 5, 7.3, 8 (except Section 8.3), 9, 10, 11, 13 and 14 will continue to apply in accordance with their terms.

(b) Post-Termination. Unless we terminate your use of the Service Offerings pursuant to Section 7.2(b), during the 30 days following the Termination Date:

(i) we will not take action to remove from the AWS systems any of Your Content as a result of the termination; and

(ii) we will allow you to retrieve Your Content from the Services only if you have paid all amounts due under this Agreement.

For any use of the Services after the Termination Date, the terms of this Agreement will apply and you will pay the applicable fees at the rates under Section 5.

8. Proprietary Rights.

8.1 Your Content. Except as provided in this Section 8, we obtain no rights under this Agreement from you (or your licensors) to Your Content. You consent to our use of Your Content to provide the Service Offerings to you and any End Users.

8.2 Adequate Rights. You represent and warrant to us that: (a) you or your licensors own all right, title, and interest in and to Your Content and Suggestions; (b) you have all rights in Your Content and Suggestions necessary to grant the rights contemplated by this Agreement; and (c) none of Your Content or End Users' use of Your Content or the Service Offerings will violate the Acceptable Use Policy.

8.3 Intellectual Property License. The Intellectual Property License applies to your use of AWS Content and the Services.

8.4 Restrictions. Neither you nor any End User will use the Service Offerings in any manner or for any purpose other than as expressly permitted by this Agreement. Neither you nor any End User will, or will attempt to (a) reverse engineer, disassemble, or decompile the Services or AWS Content or apply any other process or procedure to derive the source code of any software included in the Services or AWS Content (except to the extent applicable law doesn't allow this restriction), (b) access or use the Services or AWS Content in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (c) resell the Services or AWS Content. The AWS Trademark Guidelines apply to your use of the AWS Marks. You will not misrepresent or embellish the relationship between us and you (including by expressing or implying that we support, sponsor, endorse, or contribute to you or your business endeavors). You will not imply any relationship or affiliation between us and you except as expressly permitted by this Agreement.

8.5 Suggestions. If you provide any Suggestions to us or our affiliates, we and our affiliates will be entitled to use the Suggestions without restriction. You hereby irrevocably assign to

us all right, title, and interest in and to the Suggestions and agree to provide us any assistance we require to document, perfect, and maintain our rights in the Suggestions.

9. Indemnification.

9.1 General. You will defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives from and against any Losses arising out of or relating to any third-party claim concerning: (a) your or any End Users' use of the Service Offerings (including any activities under your AWS account and use by your employees and personnel); (b) breach of this Agreement or violation of applicable law by you, End Users or Your Content; or (c) a dispute between you and any End User. You will reimburse us for reasonable attorneys' fees, as well as our employees' and contractors' time and materials spent responding to any third party subpoena or other compulsory legal order or process associated with third party claims described in (a) through (c) above at our then-current hourly rates.

9.2 Intellectual Property.

(a) Subject to the limitations in this Section 9, AWS will defend you and your employees, officers, and directors against any third-party claim alleging that the Services infringe or misappropriate that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

(b) Subject to the limitations in this Section 9, you will defend AWS, its affiliates, and their respective employees, officers, and directors against any third-party claim alleging that any of Your Content infringes or misappropriates that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

(c) Neither party will have obligations or liability under this Section 9.2 arising from infringement by combinations of the Services or Your Content, as applicable, with any other product, service, software, data, content or method. In addition, AWS will have no obligations or liability arising from your or any End User's use of the Services after AWS has notified you to discontinue such use. The remedies provided in this Section 9.2 are the sole and exclusive remedies for any third-party claims of infringement or misappropriation of intellectual property rights by the Services or by Your Content.

(d) For any claim covered by Section 9.2(a), AWS will, at its election, either: (i) procure the rights to use that portion of the Services alleged to be infringing; (ii) replace the alleged infringing portion of the Services with a non-infringing alternative; (iii) modify the alleged infringing portion of the Services to make it non-infringing; or (iv) terminate the allegedly infringing portion of the Services or this Agreement.

9.3 Process. The obligations under this Section 9 will apply only if the party seeking defense or indemnity: (a) gives the other party prompt written notice of the claim; (b)

permits the other party to control the defense and settlement of the claim; and (c) reasonably cooperates with the other party (at the other party's expense) in the defense and settlement of the claim. In no event will a party agree to any settlement of any claim that involves any commitment, other than the payment of money, without the written consent of the other party.

10. Disclaimers.

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." EXCEPT TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, WE AND OUR AFFILIATES AND LICENSORS (A) MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD-PARTY CONTENT, AND (B) DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (I) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (II) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (III) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, AND (IV) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR ALTERED.

11. Limitations of Liability.

WE AND OUR AFFILIATES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SERVICE LEVEL AGREEMENTS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (C) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, EXCEPT FOR PAYMENT OBLIGATIONS UNDER SECTION 9.2, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL NOT EXCEED THE AMOUNT YOU ACTUALLY PAY US UNDER THIS

AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE. THE LIMITATIONS IN THIS SECTION 11 APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

12. Modifications to the Agreement.

We may modify this Agreement (including any Policies) at any time by posting a revised version on the AWS Site or by otherwise notifying you in accordance with Section 13.10; provided, however, that we will provide at least 90 days' advance notice in accordance with Section 13.10 for adverse changes to any Service Level Agreement. Subject to the 90 day advance notice requirement with respect to adverse changes to Service Level Agreements, the modified terms will become effective upon posting or, if we notify you by email, as stated in the email message. By continuing to use the Service Offerings after the effective date of any modifications to this Agreement, you agree to be bound by the modified terms. It is your responsibility to check the AWS Site regularly for modifications to this Agreement. We last modified this Agreement on the date listed at the end of this Agreement.

13. Miscellaneous.

13.1 Assignment. You will not assign or otherwise transfer this Agreement or any of your rights and obligations under this Agreement, without our prior written consent. Any assignment or transfer in violation of this Section 13.1 will be void. We may assign this Agreement without your consent (a) in connection with a merger, acquisition or sale of all or substantially all of our assets, or (b) to any affiliate or as part of a corporate reorganization; and effective upon such assignment, the assignee is deemed substituted for AWS as a party to this Agreement and AWS is fully released from all of its obligations and duties to perform under this Agreement. Subject to the foregoing, this Agreement will be binding upon, and inure to the benefit of the parties and their respective permitted successors and assigns.

13.2 Entire Agreement. This Agreement incorporates the Policies by reference and is the entire agreement between you and us regarding the subject matter of this Agreement. This Agreement supersedes all prior or contemporaneous representations, understandings, agreements, or communications between you and us, whether written or verbal, regarding the subject matter of this Agreement (but does not supersede prior commitments to purchase Services such as Amazon EC2 Reserved Instances). We will not be bound by, and specifically object to, any term, condition or other provision that is different from or in addition to the provisions of this Agreement (whether or not it would materially alter this Agreement) including for example, any term, condition or other provision (a) submitted by you in any order, receipt, acceptance, confirmation, correspondence or other document, (b) related to any online registration, response to any Request for Bid, Request for Proposal, Request for Information, or other questionnaire, or (c) related to any invoicing process that you submit or require us to complete. If the terms of this document are inconsistent with the terms contained in any Policy, the terms contained in this document will control, except that the Service Terms will control over this document.

13.3 Force Majeure. We and our affiliates will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, electrical or power outages, utilities or other telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

13.4 Governing Law. The Governing Laws, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between you and us. The United Nations Convention for the International Sale of Goods does not apply to this Agreement.

13.5 Disputes. Any dispute or claim relating in any way to your use of the Service Offerings, or to any products or services sold or distributed by AWS will be adjudicated in the Governing Courts, and you consent to exclusive jurisdiction and venue in the Governing Courts, subject to the additional provisions below.

(a) If the applicable AWS Contracting Party is Amazon Web Services, Inc., Amazon Web Services Canada, Inc., Amazon Web Services Korea LLC or Amazon Web Services Singapore Private Limited, the parties agree that the provisions of this Section 13.5(a) will apply. Disputes will be resolved by binding arbitration, rather than in court, except that you may assert claims in small claims court if your claims qualify. The Federal Arbitration Act and federal arbitration law apply to this Agreement, except that if Amazon Web Services Canada, Inc. is the applicable AWS Contracting Party the Ontario Arbitration Act will apply to this Agreement. There is no judge or jury in arbitration, and court review of an arbitration award is limited. However, an arbitrator can award on an individual basis the same damages and relief as a court (including injunctive and declaratory relief or statutory damages), and must follow the terms of this Agreement as a court would. To begin an arbitration proceeding, you must send a letter requesting arbitration and describing your claim to our registered agent Corporation Service Company, 300 Deschutes Way SW, Suite 304, Tumwater, WA 98501. The arbitration will be conducted by the American Arbitration Association (AAA) under its rules, which are available at www.adr.org or by calling 1-800-778-7879. Payment of filing, administration and arbitrator fees will be governed by the AAA's rules. We will reimburse those fees for claims totaling less than $10,000 unless the arbitrator determines the claims are frivolous. We will not seek attorneys' fees and costs in arbitration unless the arbitrator determines the claims are frivolous. You may choose to have the arbitration conducted by telephone, based on written submissions, or at a mutually agreed location. We and you agree that any dispute resolution proceedings will be conducted only on an individual basis and not in a class, consolidated or representative action. If for any reason a claim proceeds in court rather than in arbitration we and you waive any right to a jury trial. Notwithstanding the foregoing we and you both agree that you or we may bring suit in court to enjoin infringement or other misuse of intellectual property rights.

(b) If the applicable AWS Contracting Party is Amazon Web Services South Africa Proprietary Limited, the parties agree that the provisions of this Section 13.5(b) will apply.

Disputes will be resolved by arbitration in accordance with the then-applicable rules of the Arbitration Foundation of Southern Africa, and judgment on the arbitral award must be entered in the Governing Court. The Arbitration Act, No. 42 of 1965 applies to this Agreement. The arbitration will take place in Johannesburg. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties.

(c) If the applicable AWS Contracting Party is Amazon AWS Serviços Brasil Ltda., the parties agree that the provisions of this Section 13.5(c) will apply. Disputes will be resolved by binding arbitration, rather than in court, in accordance with the then-applicable Rules of Arbitration of the International Chamber of Commerce, and judgment on the arbitral award may be entered in any court having jurisdiction. The arbitration will take place in the City of São Paulo, State of São Paulo, Brazil. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties. The parties agree that the existence of and information relating to any such arbitration proceedings will not be disclosed by either party and will constitute confidential information. The Governing Courts will have exclusive jurisdiction for the sole purposes of (i) ensuring the commencement of the arbitral proceedings; and (ii) granting conservatory and interim measures prior to the constitution of the arbitral tribunal.

(d) If the applicable AWS Contracting Party is Amazon Web Services Australia Pty Ltd, the parties agree that the provisions of this Section 13.5(d) will apply. Disputes will be resolved by arbitration administered by the Australian Center for International Commercial Arbitration ("ACICA") in accordance with the then-applicable ACICA Arbitration Rules, and judgment on the arbitral award may be entered in any court having jurisdiction. The arbitration will take place in Sydney, Australia. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties. The parties agree that the existence of and information relating to any such arbitration proceedings will not be disclosed by either party and will constitute confidential information.

(e) If the applicable AWS Contracting Party is Amazon Web Services New Zealand Limited, the parties agree that the provisions of this Section 13.5(e) will apply. Disputes will be resolved by arbitration administered by the New Zealand Dispute Resolution Centre ("NZDRC") in accordance with the then-applicable Arbitration Rules of NZDRC, and judgment on the arbitral award may be entered in any court having jurisdiction. The arbitration will take place in Auckland, New Zealand. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties. The parties agree that the existence of and information relating to any such arbitration proceedings will not be disclosed by either party and will constitute confidential information.

13.6 Trade Compliance. In connection with this Agreement, each party will comply with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations, including all such laws and regulations that apply to a U.S. company, such as the Export Administration Regulations, the International Traffic in Arms Regulations, and economic sanctions programs implemented by the Office of Foreign Assets Control. For clarity, you are solely responsible for compliance related to the manner in which you choose to use the Service Offerings, including your transfer and processing of Your Content, the provision of Your Content to End Users, and the AWS region in which any of the foregoing occur. You represent and warrant that you and your financial institutions, or any party that owns or controls you or your financial institutions, are not subject to sanctions or otherwise designated on any list of prohibited or restricted parties, including but not limited to the lists maintained by the United Nations Security Council, the U.S. Government (e.g., the Specially Designated Nationals List and Foreign Sanctions Evaders List of the U.S. Department of Treasury, and the Entity List of the U.S. Department of Commerce), the European Union or its Member States, or other applicable government authority.

13.7 Independent Contractors; Non-Exclusive Rights. We and you are independent contractors, and this Agreement will not be construed to create a partnership, joint venture, agency, or employment relationship. Neither party, nor any of their respective affiliates, is an agent of the other for any purpose or has the authority to bind the other. Both parties reserve the right (a) to develop or have developed for it products, services, concepts, systems, or techniques that are similar to or compete with the products, services, concepts, systems, or techniques developed or contemplated by the other party, and (b) to assist third party developers or systems integrators who may offer products or services which compete with the other party’s products or services.

13.8 Language. All communications and notices made or given pursuant to this Agreement must be in the English language. If we provide a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

13.9 Confidentiality and Publicity. You may use AWS Confidential Information only in connection with your use of the Service Offerings as permitted under this Agreement. You will not disclose AWS Confidential Information during the Term or at any time during the 5year period following the end of the Term. You will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of AWS Confidential Information, including, at a minimum, those measures you take to protect your own confidential information of a similar nature. You will not issue any press release or make any other public communication with respect to this Agreement or your use of the Service Offerings.

13.10 Notice.

(a) To You. We may provide any notice to you under this Agreement by: (i) posting a notice on the AWS Site; or (ii) sending a message to the email address then associated with your account. Notices we provide by posting on the AWS Site will be effective upon posting and notices we provide by email will be effective when

we send the email. It is your responsibility to keep your email address current. You will be deemed to have received any email sent to the email address then associated with your account when we send the email, whether or not you actually receive the email.

(b) To Us. To give us notice under this Agreement, you must contact AWS by facsimile transmission or personal delivery, overnight courier or registered or certified mail to the facsimile number or mailing address, as applicable, listed for the applicable AWS Contracting Party in Section 14 below. We may update the facsimile number or address for notices to us by posting a notice on the AWS Site. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided registered or certified mail will be effective three business days after they are sent.

13.11 No Third-Party Beneficiaries. Except as set forth in Section 9, this Agreement does not create any third-party beneficiary rights in any individual or entity that is not a party to this Agreement.

13.12 U.S. Government Rights. The Service Offerings are provided to the U.S. Government as “commercial items,” “commercial computer software,” “commercial computer software documentation,” and “technical data” with the same rights and restrictions generally applicable to the Service Offerings. If you are using the Service Offerings on behalf of the U.S. Government and these terms fail to meet the U.S. Government’s needs or are inconsistent in any respect with federal law, you will immediately discontinue your use of the Service Offerings. The terms “commercial item” “commercial computer software,” “commercial computer software documentation,” and “technical data” are defined in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

13.13 No Waivers. The failure by us to enforce any provision of this Agreement will not constitute a present or future waiver of such provision nor limit our right to enforce such provision at a later time. All waivers by us must be in writing to be effective.

13.14 Severability. If any portion of this Agreement is held to be invalid or unenforceable, the remaining portions of this Agreement will remain in full force and effect. Any invalid or unenforceable portions will be interpreted to effect and intent of the original portion. If such construction is not possible, the invalid or unenforceable portion will be severed from this Agreement but the rest of the Agreement will remain in full force and effect.

13.15 Account Country Specific Terms. You agree to the following modifications to the Agreement that apply to your AWS Contracting Party as described below:

(a) If the applicable AWS Contracting Party is Amazon Web Services Australia Pty Ltd, the parties agree as follows:

If the Services are subject to any statutory guarantees under the Australian Competition and Consumer Act 2010, then to the extent that any part of this Agreement is unenforceable under such Act, you agree that a fair and reasonable remedy to you will be limited to, at our election, either: (i) supplying the Services again; or (ii) paying for the cost of having the Services supplied again.

(b) If the applicable AWS Contracting Party is Amazon Web Services Japan G.K., the parties agree as follows:

(i) The following sentence is added at the end of Section 8.5 (Suggestions):

"The foregoing assignment includes the assignment of the rights provided under Article 27 (Rights of Translation, Adaptation, etc.) and Article 28 (Right of the Original Author in the Exploitation of a Derivative Work) of the Copyright Act of Japan, and you agree not to exercise your moral rights against us, our affiliates or persons who use the Suggestions through the consent of us or our affiliates."

(ii) The following sentences are added at the end of Section 11 (Limitation of Liability):

"THE DISCLAIMER OR THE DAMAGES CAP IN THIS SECTION MAY NOT BE APPLIED TO DAMAGES CAUSED BY EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT IF SUCH DISCLAIMER OR THE DAMAGES CAP ARE DEEMED AGAINST PUBLIC POLICY UNDER ARTICLE 90 OF THE CIVIL CODE. IN THAT EVENT, THE SCOPE OF THE DISCLAIMER SHALL BE NARROWLY CONSTRUED IN SUCH MANNER AND THE DAMAGES CAP MAY BE INCREASED BY SUCH MINIMUM AMOUNT SO THAT THE DISCLAIMER OR THE DAMAGES CAP HEREUNDER WOULD NOT BE DEEMED AGAINST PUBLIC POLICY UNDER ARTICLE 90 OF THE CIVIL CODE."

14. Definitions.

"Acceptable Use Policy" means the policy located at http://aws.amazon.com/aup (and any successor or related locations designated by us), as it may be updated by us from time to time.

"Account Country" is the country associated with your account. If you have provided a valid tax registration number for your account, then your Account Country is the country associated with your tax registration. If you have not provided a valid tax registration, then your Account Country is the country where your billing address is located, except if you have a credit card associated with your AWS account that is issued in a different country and your contact address is also in that country, then your Account Country is that different country.

"Account Information" means information about you that you provide to us in connection with the creation or administration of your AWS account. For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with your AWS account.

“API” means an application program interface.

“AWS Confidential Information” means all nonpublic information disclosed by us, our affiliates, business partners or our or their respective employees, contractors or agents that is designated as confidential or that, given the nature of the information or circumstances surrounding its disclosure, reasonably should be understood to be confidential. AWS Confidential Information includes: (a) nonpublic information relating to our or our affiliates or business partners’ technology, customers, business plans, promotional and marketing activities, finances and other business affairs; (b) third-party information that we are obligated to keep confidential; and (c) the nature, content and existence of any discussions or negotiations between you and us or our affiliates. AWS Confidential Information does not include any information that: (i) is or becomes publicly available without breach of this Agreement; (ii) can be shown by documentation to have been known to you at the time of your receipt from us; (iii) is received from a third party who did not acquire or disclose the same by a wrongful or tortious act; or (iv) can be shown by documentation to have been independently developed by you without reference to the AWS Confidential Information.

“AWS Content” means Content we or any of our affiliates make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; Documentation; sample code; software libraries; command line tools; proofs of concept; templates; and other related technology (including any of the foregoing that are provided by our personnel). AWS Content does not include the Services or Third-Party Content.

"AWS Contracting Party" means the party identified in the table below, based on your Account Country. If you change your Account Country to one identified to a different AWS Contracting Party below, you agree that this Agreement is then assigned to the new AWS Contracting Party under Section 13.1 without any further action required by either party.

Account Country	AWS Contracting Party	Facsimile	Mailing Address
Australia	Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891)	N/A	Level 37, 2-26 Park Street, Sydney, NSW, 2000, Australia
Brazil*	Amazon AWS Serviços Brasil Ltda.	N/A	A. Presidente Juscelino Kubitschek, 2.041, Torre E - 18th and 19th Floors, Vila Nova Conceicao, São Paulo, Brasil

Canada	Amazon Web Services Canada, Inc.	N/A	120 Bremner Blvd, 26th Floor, Toronto, Ontario, M5J 0A8, Canada
Japan	Amazon Web Services Japan G.K.	N/A	1-1, Kamiosaki 3-chome, Shinagawa-ku, Tokyo, 141-0021, Japan
New Zealand	Amazon Web Services New Zealand Limited	N/A	Level 5, 18 Viaduct Harbour Ave, Auckland, 1010, New Zealand
Singapore	Amazon Web Services Singapore Private Limited	N/A	23 Church Street, #10-01, Singapore 049481
South Africa	Amazon Web Services South Africa Proprietary Limited	206-266-7010	Wembley Square 2, 134 Solan Road, Gardens, Cape Town, 8001, South Africa
South Korea	Amazon Web Services Korea LLC	N/A	L12, East tower, 231, Teheran-ro, Gangnam-gu, Seoul, 06142, Republic of Korea
Any country within Europe, the Middle East, or Africa (excluding South Africa) ("EMEA")**	Amazon Web Services EMEA SARL	352 2789 0057	38 Avenue John F. Kennedy, L-1855, Luxembourg
Any country that is not listed in this table above.	Amazon Web Services, Inc.	206-266-7010	410 Terry Avenue North, Seattle, WA 98109-5210 U.S.A.

*Brazil is your Account Country only if you have provided a valid Brazilian Tax Registration Number (CPF/CNPJ number) for your account. If your billing address is located in Brazil but you have not provided a valid Brazilian Tax Registration Number (CPF/CNPJ number), then Amazon Web Services, Inc. is the AWS Contracting Party for your account.

**See https://aws.amazon.com/legal/aws-emea-countries for a full list of EMEA countries.

“AWS Marks” means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its affiliates that we may make available to you in connection with this Agreement.

“AWS Site” means http://aws.amazon.com (and any successor or related site designated by us), as may be updated by us from time to time.

“AWS Trademark Guidelines” means the guidelines and trademark license located at http://aws.amazon.com/trademark-guidelines/ (and any successor or related locations designated by us), as they may be updated by us from time to time.

“Content” means software (including machine images), data, text, audio, video or images.

“Documentation” means the user guides and admin guides (in each case exclusive of content referenced via hyperlink) for the Services located at http://aws.amazon.com/documentation (and any successor or related locations designated by us), as such user guides and admin guides may be updated by AWS from time to time.

“End User” means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under your account. The term “End User” does not include individuals or entities when they are accessing or using the Services or any Content under their own AWS account, rather than under your account.

"Governing Laws" and “Governing Courts” mean, for each AWS Contracting Party, the laws and courts set forth in the following table:

AWS Contracting Party	Governing Laws	Governing Courts
Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891)	The laws of New South Wales	The courts of New South Wales
Amazon AWS Serviços Brasil Ltda.	The laws of Brazil	The courts of the City of São Paulo, State of São Paulo
Amazon Web Services Canada, Inc.	The laws of the Province of Ontario, Canada and federal	The provincial or federal courts located in Toronto, Ontario, Canada.

	laws of Canada applicable therein.	
Amazon Web Services EMEA SARL	The laws of the Grand Duchy of Luxembourg	The courts in the district of Luxembourg City
Amazon Web Services, Inc.	The laws of the State of Washington	The state or Federal courts in King County, Washington
Amazon Web Services Japan G.K.	The laws of Japan	The Tokyo District Court
Amazon Web Services Korea LLC	The laws of the State of Washington	The state or Federal courts in King County, Washington
Amazon Web Services New Zealand Limited	The laws of New Zealand	The courts of New Zealand
Amazon Web Services Singapore Private Limited	The laws of the State of Washington	The state or Federal courts in King County, Washington
Amazon Web Services South Africa Proprietary Limited	The laws of the Republic of South Africa	The South Gauteng High Court, Johannesburg

“Indirect Taxes” means applicable taxes and duties, including, without limitation, VAT, Service Tax, GST, excise taxes, sales and transactions taxes, and gross receipts tax.

“Intellectual Property License” means the separate license terms that apply to your access to and use of AWS Content and Services located at https://aws.amazon.com/legal/aws-ip-license-terms (and any successor or related locations), as may be updated from time to time.

“Losses” means any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys’ fees).

“Policies” means the Acceptable Use Policy, Privacy Notice, the Site Terms, the Service Terms, the AWS Trademark Guidelines, all restrictions described in the AWS Content and on the AWS Site, and any other policy or terms referenced in or incorporated into this Agreement, but does not include whitepapers or other marketing materials referenced on the AWS Site.

“Privacy Notice” means the privacy notice located at http://aws.amazon.com/privacy (and any successor or related locations designated by us), as it may be updated by us from time to time.

“Service” means each of the services made available by us or our affiliates, including those web services described in the Service Terms. Services do not include Third-Party Content.

"Service Level Agreement" means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time. The service level agreements we offer with respect to the Services are located at https://aws.amazon.com/legal/service-level-agreements/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"Service Offerings" means the Services (including associated APIs), the AWS Content, the AWS Marks, and any other product or service provided by us under this Agreement. Service Offerings do not include Third-Party Content.

"Service Terms" means the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms (and any successor or related locations designated by us), as may be updated by us from time to time.

"Site Terms" means the terms of use located at http://aws.amazon.com/terms/ (and any successor or related locations designated by us), as may be updated by us from time to time.

"Suggestions" means all suggested improvements to the Service Offerings that you provide to us.

"Term" means the term of this Agreement described in Section 7.1.

"Termination Date" means the effective date of termination provided in accordance with Section 7, in a notice from one party to the other.

"Third-Party Content" means Content made available to you by any third party on the AWS Site or in conjunction with the Services.

"Your Content" means Content that you or any End User transfers to us for processing, storage or hosting by the Services in connection with your AWS account and any computational results that you or any End User derive from the foregoing through their use of the Services. For example, Your Content includes Content that you or any End User stores in Amazon Simple Storage Service. Your Content does not include Account Information.

Appendix 1 to the AWS Customer Agreement – AWS Enterprise Support Additional Terms and Conditions

THE FOLLOWING AWS ENTERPRISE SUPPORT TERMS AND CONDITIONS SHALL APPLY TO EACH CALL-OFF CONTRACT ISSUED UNDER THE G-CLOUD 13 FRAMEWORK AGREEMENT WHERE THE BUYER HAS SUBSCRIBED TO ENTERPRISE – LEVEL AWS SUPPORT.

AWS ENTERPRISE SUPPORT ADDITIONAL SUPPLIER TERMS

The following is included as additional Supplier Terms where Buyer has executed a CallOff Contract to procure Enterprise-level AWS Support, including where Enterprise Support is included in the offering (e.g. The UKGDP Program and/or AWS Managed Services). Enterprise-level AWS Support provides Buyer with one-on-one Technical Support services to help Buyers business utilize the products and features provided by Amazon Web Services.

To subscribe for Enterprise-level AWS Support pursuant to the G-Cloud Call-Off Agreement following execution of the Call-Off Contract, Supplier requires the AWS account numbers that Buyer intends to enroll to enable this service. Buyer will notify the account ID(s) to Supplier at aws-gcloud@amazon.com.

AWS ACCOUNTS

These additional terms and conditions will cover the account(s) notified to Supplier at awsgcloud@amazon.com and other all accounts linked to the account(s) listed above via Consolidated Billing, provided that all such linked accounts are opened by Buyer or Buyers employees using email addresses issued by Buyer, for use by Buyer or Buyers employees:

(1) Accounts may be added to or removed by mutual agreement of the parties (which agreement may be made via email.)

(2) For those accounts notified to Supplier, Supplier will provide AWS Support at the Enterprise subscription level to Buyer in accordance with the terms and Enterprise-level pricing located on the Digital Marketplace and the AWS Support Service Terms at http://aws.amazon.com/serviceterms/ . These terms form part of the "Supplier Terms" of the G-Cloud Call-Off Agreement and therefore are incorporated into the Call-Off Agreement.

(3) Buyer will be billed for AWS Support on a monthly basis and payments for AWS Support are non-refundable. If Buyer cancels their subscription within 30 days of sign up

Buyer will see a minimum subscription charge on their next bill. All other terms and conditions of the G-Cloud Call-Off Agreement shall apply.

Appendix 2 – GDPR Data Processing Addendum

THE FOLLOWING AWS GDPR DATA PROCESSING ADDENDUM (AS SUPPLENTED BY THE UK GDPR ADDENDUM IN ANNEX 3 AND THE SUPPLEMENTARY ADDENDUM TO AWS GDPR DATA PROCESSING ADDENDUM IN ANNEX 4) SHALL APPLY TO EACH CALL-OFF ISSUED UNDER THE G-CLOUD 13 FRAMEWORK AGREEMENT WHERE THE CUSTOMER HAS IDENTIFIED TO THE SUPPLIER THAT IT MUST COMPLY WITH THE DATA PROTECTION LEGISLATION AND/OR INTENDS TO TRANSFER DATA OUTSIDE THE EEA

AWS GDPR 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 Service Offerings (the "**Agreement**") when the GDPR applies to your use of the AWS Services to process Customer Data. 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 capitalised 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 the GDPR, 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 the GDPR.

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

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

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

(c) measures to control access rights for AWS employees and contractors to the AWS Network as set out in Section 1.1 of the AWS Security Standards; and

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

5.2 Customer can elect to implement technical and organisational measures to protect Customer Data. Such technical and organisational 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) pseudonymisation 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;

(c) 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

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

6. Sub-processing.

6.1 **Authorised Sub-processors.** Customer provides general authorisation 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 AWS Region where AWS has not engaged the Sub-processor.

6.2 **Sub-processor Obligations.** Where AWS authorises 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 the GDPR. 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 authorises 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 unauthorised 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 unauthorised 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 unauthorised 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 the GDPR 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 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 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 recognised 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 capitalised terms used in this DPA will have the meanings given to them below:

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

"**AWS Security Standards**" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Annex 1.

"**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 the GDPR) that is uploaded to the Services under Customer's AWS accounts.

"**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.

"**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.

"**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 recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1

AWS Security Standards

Capitalised 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 (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access

privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. **Continued Evaluation.** AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Annex 2

Minimum Architecture Requirements

Customer agrees and acknowledges that that it will issue all necessary instructions via the AWS console, and take all other necessary actions, to implement at least the minimum architecture requirements specified below. Each reference in this Attachment to specific Services includes equivalent alternative or replacement Service(s) that AWS makes available. At all times Customer will comply with all of the following:

1. **Encryption.**
   (a) Encrypt all Customer Content in transit and at rest, using Strong Cryptography with associated key management processes and procedures. "**Strong Cryptography**" has the meaning given in Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms, Version 3.2 (as updated from time to time).
   (b) Ensure that it will not utilize unencrypted Customer Content as metadata or as parameters for configuring Services.
   (c) Ensue that it will not store unencrypted Customer Content as part of an Amazon Machine Image ("**AMI**").
   (d) Ensure that it will not store account credentials as part of an AMI.
2. **Security Architecture.**
   (a) Promptly address any security and privacy events as notified at http://aws.amazon.com/security/security-bulletins/, except those categorized as "Informational".
   (b) Monitor and evaluate software running in its AWS Enterprise Accounts for known and new vulnerabilities and take the steps necessary to address such vulnerabilities.
   (c) Configure AWS CloudTrail where available for all Services and implement appropriate retention, monitoring, and incident response processes using AWS CloudTrail logs.
   (d) Enable and configure Service-specific logging features where available for all Services and implement appropriate monitoring and incident response processes. For example, without limitation, where appropriate, Customer will enable access request logging features in Amazon Elastic Load Balancing, access request logging features in Amazon S3, database logging in Amazon Relational Database Service, and other logging features available in the Services.

(e) Apply appropriate resource-based policies limiting access only to authorized parties to all Services where available.

3. Access Management.

(a) Use multi-factor authentication to control access to root account credentials and not use root account credentials beyond initial account configuration, except in using Services for which AWS Identity and Access Management (IAM) is not available.

(b) Require each user to have unique security credentials that are rotated at least quarterly.

(c) Use multifactor authentication or federated credentials for all authentications and grant users and groups only the minimum privileges necessary.

(d) Restrict permissions in Security Groups and Access Control Lists to only those users required for Customer's use of the Services.

(e) Restrict permitted source and destination authorizations to only those required for Customer's use of the Services.

(f) Apply resource-based policies to limit access to Services only to authorized parties.

4. Backup and Redundancy.

(a) Back up Customer Content in accordance with industry-standard security configurations.

(b) Store Customer Content redundantly in more than one AWS Region

Annex 3

UK GDPR Addendum

This UK GDPR Addendum (this "UK **Addendum**") supplements the AWS GDPR Data Processing Addendum set out in Appendix 2 (the "**AWS GDPR DPA**"). This UK Addendum applies when the UK GDPR applies to Customer's use of the Services to process UK Customer Data. Unless otherwise defined in this UK Addendum, all capitalised terms used in this UK Addendum will have the meanings given to them in the AWS GDPR DPA.

1. **Applicability.** Except as otherwise set out in this UK Addendum, the terms of the AWS GDPR DPA will apply to Customer's use of the Services to process UK Customer Data, and all references to "GDPR" in the AWS GDPR DPA will be replaced with "UK GDPR", all references to "Customer Data" in the AWS GDPR DPA will be replaced with "UK Customer Data", and all references to "Standard Contractual Clauses" will be replaced with "Legacy Standard Contractual Clauses".

2. **Transfers of UK Customer Data.** When this UK Addendum applies, Sections 12.2 ("Application of Standard Contractual Clauses") and 12.3 ("Alternative Transfer Mechanism") of the AWS GDPR DPA will not apply, and the following Section will apply:

"**Application of Legacy Standard Contractual Clauses**. The Legacy Standard Contractual Clauses will only apply to UK Customer Data that is transferred, either directly or via onward transfer, to any UK Third Country (each a "**UK Data Transfer**"). The Legacy Standard Contractual Clauses will not apply to a UK Data Transfer if AWS has adopted an alternative recognised compliance standard for lawful UK Data Transfers."

3. **Definitions.** The following capitalised terms used in this UK Addendum have the meaning given to them below:

""**Legacy Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to processors established in third countries as approved by the European Commission Decision of 5 February 2010, and currently located in Annex 5.

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

"**UK GDPR**" means the GDPR as amended and incorporated into UK law under the European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

"**UK Third Country**" means a country outside the UK not recognised by the Secretary of State or the Data Protection Act 2018 as providing an adequate level of protection for personal data (as described in the UK GDPR)."

4. **Legacy Standard Contractual Clauses.** Annex 5 ("Standard Contractual Clauses (processors)") will apply in accordance with Section 2 of this UK Addendum.

5. **Entire Agreement; Conflict.** Except as supplemented by this UK Addendum and the Supplementary Addendum, the AWS GDPR DPA (if applicable) and the Agreement will remain in full force and effect. Where this UK Addendum and/or the Supplementary Addendum and/or the AWS GDPR DPA apply to a processing activity, all will apply concurrently (as applicable). This UK Addendum, together with the Supplementary Addendum, the AWS GDPR DPA and the Agreement: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof.

Annex 4

Supplementary Addendum to AWS GDPR Data Processing Addendum

The purpose of this supplementary addendum (this **"Supplementary Addendum")** is to outline supplemental measures that AWS takes to protect Customer Data. This Supplementary Addendum supplements, but does not modify, the AWS GDPR Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-gdpr/AWS GDPR DPA.pdf. or other agreement between Customer and AWS governing the processing of Customer Data pursuant to the GDPR (the **"AWS GDPR DPA**")**.** Unless otherwise defined in this Supplementary Addendum, all capitalised terms used in this Supplementary Addendum will have the meanings given to them in the AWS GDPR DPA.

1. Requests for Customer Data

1.1 If AWS receives a valid and binding order ("**Request**") from any governmental body ("**Requesting Party**") for disclosure of Customer Data, AWS will use every reasonable effort to redirect the Requesting Party to request Customer Data directly from Customer.

1.2 If compelled to disclose Customer Data to a Requesting Party, AWS will:

(a) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so. If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible; and

(b) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union or applicable Member State law).

1.3 If, after exhausting the steps described in Section 1.2, AWS remains compelled to disclose Customer Data to a Requesting Party, AWS will disclose only the minimum amount of Customer Data necessary to satisfy the Request.

2. Data Subject Rights. Nothing in this Supplementary Addendum restricts Customer's data subjects from exercising their rights under the GDPR, including their rights to compensation from AWS for material or non-material damage under, and in accordance with, Article 82 of the GDPR.

3. Warranty. AWS agrees and warrants that it has no reason to believe that the legislation applicable to it, or its sub-processors, including in any country to which Customer Data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from Customer and its obligations under this Supplementary Addendum and the AWS GDPR DPA and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the

warranties and obligations provided by this Supplementary Addendum and the AWS GDPR DPA, AWS will promptly notify the change to Customer as soon as AWS is aware, in which case Customer is entitled to suspend the transfer of Customer Data and/or terminate the Agreement.

4. **Entire Agreement; Conflict.** Except as supplemented by this Supplementary Addendum and the UK Addendum, the AWS GDPR DPA and the Agreement will remain in full force and effect. This Supplementary Addendum, together with the UK Addendum, AWS GDPR DPA and the Agreement: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof. Where this Supplementary Addendum and/or the UK Addendum and/or the AWS GDPR DPA apply to a processing activity, all will apply concurrently (as applicable). If there is a conflict between the AWS GDPR DPA, the UK Addendum and/or this Supplementary Addendum, the terms of this Supplementary Addendum will control.

Annex 5

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity defined as “Customer” in the AWS GDPR DPA
(the “**data exporter**”)

And

“AWS”, as defined in the AWS GDPR DPA
(the “**data importer**”)

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

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the

contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or

subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall

remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity defined as “Customer” in the AWS GDPR DPA.

Data importer

The data importer is “AWS”, as defined in the AWS GDPR DPA.

Data subjects

Data subjects are defined in Section 1.3 of the AWS GDPR DPA.

Categories of data

The personal data is defined in Section 1.3 of the AWS GDPR DPA.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing operations are defined in Section 1.3 of the AWS GDPR DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures implemented by the data importer are as described in the AWS GDPR DPA.