UK G-Cloud 14 Framework Agreement

AWS EMEA SARL, UK Branch - Supplier Terms

May 2024

Submitted By:

John Davies
Director, UK Public Sector aws-gcloud@amazon.com

Table of Contents

1.0 INTRODUCTION 3
1.1 General 3
1.2 Definition alignment 4
2.0 AWS CUSTOMER AGREEMENT 6
Appendix 1 to the AWS Customer Agreement – AWS Enterprise Support Additional Terms and Conditions 26
Appendix 2 – GDPR Data Processing Addendum 28
Annex 1 – Security Standards 38
Appendix 3 – UK GDPR Addendum 44
Appendix 4 – Supplementary Addendum to AWS GDPR Data Processing Addendum 56
Appendix 5 – Standard Contractual Clauses Controller-to Processor Transfers 58
Appendix 6 – Standard Contractual Clauses Processor-to Processor Transfers 76

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 Platform for the G-Cloud 14 Framework Agreement.

The order of precedence for these Supplier Terms is addressed in the G-Cloud 14 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 14 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 Platform.
- 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 applicable law as per the terms of the G-Cloud 14 Framework Agreement.

Should the Buyer choose to (i) purchase products or Services that are not offered on the Platform, 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 14 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 Platform, 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 14 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 Services (as defined below) and is an agreement between the applicable AWS Contracting Party specified in Section 12 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 Services (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 12 for definitions of certain capitalized terms used in this Agreement.

1. AWS Responsibilities

1.1 General. You may access and use the Services in accordance with this Agreement. Service Level Agreements and Service Terms apply to certain Services.

1.2 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.

1.3 AWS Security. Without limiting Section 8 or your obligations under Section 2.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

1.4 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 Services, 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 1.4. 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.

1.5 Notice of Changes 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 before discontinuing a material functionality of a Service that we make generally available to customers and that you are using. AWS will not be obligated to provide such notice under this Section 1.5 if the discontinuation is necessary to (a) address an emergency, or risk of harm to the Services or AWS, (b) respond to claims, litigation, or loss of license rights related to third party intellectual property rights, or (c) comply with law, but should any of the preceding occur AWS will provide you with as much prior notice as is reasonably practicable under the circumstances.

1.6 Notice of Changes to the Service Level Agreements. We may change, discontinue or add Service Level Agreements, provided, however, that we will provide at least 90 days' advance notice for adverse changes to any Service Level Agreement.

2. Your Responsibilities.

2.1 Your Accounts. You will comply with the terms of this Agreement and all laws, rules and regulations applicable to your use of the Services. 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. 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.

2.2 Your Content. You are responsible for Your Content. You will ensure that Your Content and your and End Users' use of Your Content or the Services will not violate any of the Policies or any applicable law.

2.3 Your Security and Backup. You are responsible for properly configuring and using the Services 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, including but not limited to the Minimum Architecture Requirements, as set out in Annex II of Appendix II.

2.4 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.

2.5 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 Services. You are responsible for End Users' use of Your Content and the Services, and for their compliance with your obligations under 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 Services 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.

3. Fees and Payment.

3.1 Service Fees. We calculate and bill fees and charges monthly. We may bill you more frequently for fees accrued if we reasonably 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 Services 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. If we suspend your account under Section 4.1 or terminate your use of the Services pursuant to Section 5.2(b)(ii), we may elect not to bill you for fees and charges after suspension unless your account is reinstated.

3.2 Taxes.

(a) 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 can 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 required by law. If any such deduction or withholding (including 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.

(b) If the applicable AWS Contracting Party is Amazon Web Services India Private Limited ("AWS India") (formerly known as Amazon Internet Services Private Limited), the parties agree that the provisions of this Section 3.2(b) will apply.

You acknowledge that AWS India may display the applicable fees and charges for the Services on the Site in USD (or such other currency as AWS India may deem fit). However, AWS India will invoice you in INR calculated and converted in accordance with the conversion rate determined by us on the date of invoice ("INR Equivalent Fees"). You will only be liable to pay the INR Equivalent Fees indicated in each invoice.

We will invoice you from our registered office at the address of your establishment (as registered with the tax authorities, if applicable) receiving the Services in accordance with the applicable indirect tax laws.

All fees and charges payable under this Agreement will be exclusive of applicable national, state or local indirect taxes ("Taxes") that AWS India is legally obligated to charge under applicable law. For the purpose of this clause, local indirect taxes include Goods and Services Tax (“GST”), which includes the Central Goods and Services Tax ("CGST"), the State Goods and Services Tax ("SGST"), the Union Territory Goods and Services Tax ("UGST"), the Integrated Goods and Services Tax ("IGST") as may be applicable. The Taxes charged by AWS India will be stated in the invoice pursuant to applicable laws. AWS India may charge and you will pay any applicable Taxes, which are stated separately on the invoice. As per the statutory requirement under GST, you will provide all necessary information such as the correct GST registered address, legal name and GSTIN ("GST Information") in order for AWS India to issue correct GST invoices as per the applicable legal requirements. In the event, the GST invoice is incorrect, you will inform us in a timely manner, to enable AWS India to correct the GST tax invoice. AWS India will determine the place of supply for the Services based on the GST Information provided by you and accordingly, charge GST (CGST and SGST/UTGST or IGST) on its invoice. Any withholding taxes that may be applicable to the fees and charges payable to us are for our account. You will pay the fees and charges in our invoice in full (gross) without applying any withholding taxes. If you separately deposit applicable withholding taxes on such fees and charges to the applicable government treasury and issue us a withholding tax certificate evidencing such deposit, following receipt of the withholding tax certificate in original form, we will reimburse to you an amount equal to the taxes that are evidenced as deposited.

4. Temporary Suspension.

4.1 Generally. We may suspend your or any End User’s right to access or use any portion or all of the Services immediately upon notice to you if we reasonably determine:

(a) your or an End User’s use of the Services (i) poses a security risk to the Services or any third party, (ii) could adversely impact our systems, the Services 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 material breach of this Agreement;

(c) you are in breach of your payment obligations under Section 3; 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.

4.2 Effect of Suspension. If we suspend your right to access or use any portion or all of the Services:

(a) you will be responsible for all fees and charges you incur during the period of suspension that we bill to you; and

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

5. Term; Termination.

5.1 Term. The term of this Agreement will commence on the Effective Date and will remain in effect until terminated under this Section 5. 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 5.2.

5.2 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 4 and the issue giving us the right to suspend either:

a. is not capable of being remedied; or

b. has not been remedied within 30 days of us suspending your service under Section 4.1;

(B) if our relationship with a third-party partner who provides software or other technology we use to provide the Services 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.

5.3 Effect of Termination.

(a) Generally. Upon the Termination Date:

(i) except as provided in Sections 5.3(a)(iv) and 5.3(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 5.3(b) that we bill to you;

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

(iv) Sections 2.1, 3, 5.3, 6 (except Section 6.3), 7, 8, 9, 11 and 12 will continue to apply in accordance with their terms.

(b) Post-Termination. Unless we terminate your use of the Services pursuant to Section 5.2(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 3.

6. Proprietary Rights.

6.1 Your Content. Except as provided in this Section 6, 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 Services to you and any End Users.

6.2 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 Services will violate the Acceptable Use Policy.

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

6.4 Restrictions. Neither you nor any End User will use the AWS Content or Services 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.

6.5 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.

7. Indemnification.

7.1 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 Services (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.

7.2 Intellectual Property.

(a) Subject to the limitations in this Section 7, 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 7, 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 7.2 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 7.2 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 7.2(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.

7.3 Process. The obligations under this Section 7 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.

8. Disclaimers.

THE SERVICES AND AWS CONTENT 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 SERVICES OR AWS CONTENT 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 SERVICES OR AWS CONTENT 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.

9. Limitations of Liability.

9.1 Liability Disclaimers. EXCEPT FOR PAYMENT OBLIGATIONS UNDER SECTION 7, NEITHER AWS NOR YOU, NOR ANY OF THEIR AFFILIATES OR LICENSORS, WILL HAVE LIABILITY TO THE OTHER UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITY, FOR (A) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, (B) THE VALUE OF YOUR CONTENT, (C) LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, OR GOODWILL, OR (D) UNAVAILABILITY OF THE SERVICES OR AWS CONTENT (THIS DOES NOT LIMIT ANY SERVICE CREDITS UNDER SERVICE LEVEL AGREEMENTS).

9.2 Damages Cap. EXCEPT FOR PAYMENT OBLIGATIONS UNDER SECTION 7, THE AGGREGATE LIABILITY UNDER THIS AGREEMENT OF EITHER AWS OR YOU, AND ANY OF THEIR RESPECTIVE AFFILIATES OR LICENSORS, WILL NOT EXCEED THE AMOUNTS PAID BY YOU TO AWS UNDER THIS AGREEMENT FOR THE SERVICES THAT GAVE RISE TO THE LIABILITY DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE; EXCEPT THAT NOTHING IN THIS SECTION 9 WILL LIMIT YOUR OBLIGATION TO PAY AWS FOR YOUR USE OF THE SERVICES PURSUANT TO SECTION 3, OR ANY OTHER PAYMENT OBLIGATIONS UNDER THIS AGREEMENT.

10. 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 11.10. 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 Services or AWS Content 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 beginning of this Agreement.

11. Miscellaneous.

11.1 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 11.1 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.

11.2 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). None of the parties will be bound by 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.

11.3 Force Majeure. Except for payment obligations, neither party nor any of their affiliates will be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond its 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.

11.4 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.

11.5 Disputes. Any dispute or claim relating in any way to your use of the Services, 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 11.5(a) will apply. Disputes will be resolved by binding arbitration, rather than in court, except that either party may elect to proceed 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 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. Before you may begin an arbitration proceeding, you must send a letter notifying us of your intent to pursue 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 commercial 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 commercial fee schedule. 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. We and you further agree that the underlying award in arbitration may be appealed pursuant to the AAA's Optional Appellate Arbitration Rules. 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 11.5(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 11.5(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 11.5(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 11.5(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.

(f) If the applicable AWS Contracting Party is Amazon Web Services Malaysia Sdn. Bhd. (Registration No. 201501028710 (1154031-W)), the parties agree that the provisions of this Section 11.5(f) will apply. Disputes will be resolved by arbitration administered by the Singapore International Arbitration Centre ("SIAC") in accordance with the then-applicable Arbitration Rules of SIAC, and judgment on the arbitral award may be entered in any court having jurisdiction. The arbitration will take place in Singapore. 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.

(g) If the applicable AWS Contracting Party is AWS India, the parties agree that the provisions of this Section 11.5(g) will apply. Disputes will be resolved by binding arbitration, rather than in court. Arbitration will be conducted by a panel consisting of three (3) arbitrators, with one (1) nominated by each party and the third chosen by the two (2) arbitrators so nominated. The decision and award will be determined by the majority of the panels and shall be final and binding upon the parties. The arbitration will be conducted in accordance with the provisions of the Arbitration and Conciliation Act, 1996 of India, as may be in force from time to time. The arbitration proceedings will be conducted in English, and the seat of the arbitration will be New Delhi. The cost of the arbitration, including fees and expenses of the arbitrator, shall be shared equally by the parties, unless the award otherwise provides. The courts at New Delhi shall have the exclusive jurisdiction for all arbitral applications. The Parties agree that the existence of and information relating to any such arbitration proceedings will not be disclosed by either party. Notwithstanding the foregoing, any party may seek injunctive relief in any court of competent jurisdiction for any actual or alleged infringement of such party's, its affiliates' or any third party's intellectual property or other proprietary rights.

(h) If the applicable AWS Contracting Party is AWS Turkey Pazarlama Teknoloji ve Danışmanlık Hizmetleri Limited Şirketi, the parties agree that the provisions of this Section 11.5(h) will apply. Disputes will be resolved by arbitration administered by the International Chamber of Commerce International Court of Arbitration (the "ICC Court") in accordance with the then-applicable arbitration rules (the "ICC Rules").The arbitration proceedings will be conducted in English, and the seat of arbitration will be Zurich. There will be three arbitrators. Each party will appoint one arbitrator in accordance with the ICC Rules. Within 30 days of the appointment of the co-arbitrators, the two appointed arbitrators will appoint the third arbitrator as the president of the arbitral tribunal. If the twoappointed arbitrators fail to appoint a third arbitrator as the president within such 30 day period, then the ICC Court will appoint the president. 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.

11.6 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 Services or AWS Content, 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.

11.7 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.

11.8 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.

11.9 Confidentiality and Publicity. You may use AWS Confidential Information only in connection with your use of the Services or AWS Content as permitted under this Agreement. You will not disclose AWS Confidential Information during the Term or at any time during the 5-year 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 Services or AWS Content.

11.10 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 12 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.

11.11 No Third-Party Beneficiaries. Except as set forth in Section 7, this Agreement does not create any third-party beneficiary rights in any individual or entity that is not a party to this Agreement.

11.12 U.S. Government Rights. The Services and AWS Content 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 Services and AWS Content. If you are using the Services and AWS Content 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 Services and AWS Content. 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.

11.13 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.

11.14 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.

11.15 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:

(i) 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.

(ii) If this Agreement is a "consumer contract" or "small business contract" as defined in the Australian Competition and Consumer Act 2010:

a. Section 7.1 will not apply to the extent the applicable Losses or damages are caused by AWS's gross negligence or criminal misconduct. For these purposes, "gross negligence" means an act or omission by an employee who has authority to bind AWS that is negligent and a wilful and significant disregard of an obvious and material risk.

b. If we are required to give prior notice under Section 1.5 or Section 3, we will give you this notice by email or a reasonably substitutable alternative means. If we modify this Agreement under Section 10 in a way that is materially adverse to you (as reasonably determined by AWS), we will give you at least 30 days' prior notice of the modification by email or a reasonably substitutable alternative means.

(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 6.5 (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 9 (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."

(c) If the applicable AWS Contracting Party is AWS Turkey Pazarlama Teknoloji ve Danışmanlık Hizmetleri Limited Şirketi, the parties agree as follows:

(i) The following sentence is added at the end of Section 3.2(a) (Taxes):

"If we are required to pay any stamp tax in relation to this Agreement or any other document related to this Agreement, we may charge you and you will pay us 50% of the amounts of any stamp tax paid by us."

12. Definitions.

"Acceptable Use Policy" means the policy located at http://aws.amazon.com/aup (and any successor or related locations designated by us), as 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 APIs, WSDLs, sample code, software libraries, command line tools, proofs of concept, templates, advice, information, programs (including credit programs) and any other Content made available by us and our affiliates related to use of the Services or on the AWS Site 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 that is identified with a different AWS Contracting Party, you agree that the AWS Contracting Party identified with your new Account Country is your AWS Contracting Party, 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
India	Amazon Web Services India	011-	Unit Nos. 1401 to 1421 International

	Private Limited (formerly known as Amazon Internet Services Private Limited), having its registered office at Unit Nos. 1401 to 1421 International Trade Tower, Nehru Place, New Delhi 110019, India	47985609	Trade Tower, Nehru Place, Delhi 110019, India.
Japan	Amazon Web Services Japan G.K.	N/A	1-1, Kamiosaki 3-chome, Shinagawa-ku, Tokyo, 141-0021, Japan
Malaysia	Amazon Web Services Malaysia Sdn. Bhd. (Registration No. 201501028710 (1154031-W))	N/A	Level 26 & Level 35, The Gardens North Tower, Lingkaran Syed Putra, Mid Valley City, Kuala Lumpur, 59200, Malaysia
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
Türkiye	AWS Turkey Pazarlama Teknoloji ve Danışmanlık Hizmetleri Limited Şirketi	N/A	Esentepe Mahallesi Bahar Sk. Özdilek/River Plaza/Wyndham Grand Hotel Apt. No: 13/52 Şişli, Istanbul, 34394, Türkiye
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 locations 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 may be updated by us from time to time.

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

“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 Services 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 AWS Serviços Brasil Ltda	The laws of Brazil	The courts of the City of São Paulo, State of São Paulo
Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891)	The laws of New South Wales	The courts of New South Wales
Amazon Web Services Canada, Inc.	The laws of the Province of Ontario, Canada and federal laws of Canada applicable therein	The provincial or federal courts located in Toronto, Ontario, Canada
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 India Private Limited (AWS India)	The laws of India	The courts in New Delhi, India
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 Malaysia Sdn. Bhd. (Registration No. 201501028710 (1154031-W))	The laws of Malaysia	The courts of Malaysia
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
AWS Turkey Pazarlama Teknoloji ve Danışmanlık Hizmetleri Limited Şirketi	The laws of the Grand Duchy of Luxembourg	The courts in the district of Luxembourg City

“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 designated by us), as may be updated by us 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, and the AWS Trademark Guidelines.

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

“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 of the AWS Site 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 Services or AWS Content that you provide to us.

“Term” means the term of this Agreement described in Section 5.1.

“Termination Date” means the effective date of termination provided in a notice from one party to the other in accordance with Section 5.

“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 14 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. 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 Platform 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 14 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 DATA PROCESSING ADDENDUM

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

1. Data Processing.

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

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

1.3 Details of Data Processing.

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

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

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

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

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

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

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

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

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

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

5. Security of Data Processing

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

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

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

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

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

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

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

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

(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 organizational measures implemented by Customer.

6. Sub-processing.

6.1 **Authorized Sub-processors.** Customer provides general authorization to AWS's use of sub-processors to provide processing activities on Customer

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

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

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

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

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

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

8. Optional Security Features. AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

9. Security Incident Notification.

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

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

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

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

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

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

9.5 **Notification Obligations.** If AWS notifies Customer of a Security Incident, or Customer otherwise becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data, Customer will be responsible for (a) determining if there is any resulting notification or other obligation under Applicable Data Protection Law and (b) taking necessary action to comply with those obligations. This does not limit AWS's obligations under this Section 9.

10. AWS Certifications and Audits.

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

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

(ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

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

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

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

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

12. Transfers of Personal Data.

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

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

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

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

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

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

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

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

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

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

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

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

"**AWS Network**" means the servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS's control and are used to provide the Services. "**Binding Corporate Rules**" has the meaning given to it in the GDPR.
"**controller**" has the meaning given to it in the GDPR.

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

"**Customer Data**" means the Personal Data that is uploaded to the Services under Customer's AWS accounts.

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

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

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

"**Personal Data**" means personal data, personal information, personally identifiable information or other equivalent term (each as defined in Applicable Data Protection Law).

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

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

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

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

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

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

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

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

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

Annex 1 – Security Standards

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

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

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

1.1 Logical Security**.**

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

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

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

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

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

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

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

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

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

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

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

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

1.2 Physical Security**.**

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

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

1.3 AWS Employees.

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

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

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

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

Annex II- 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

Appendix 3 – UK GDPR Addendum

This UK GDPR Addendum (this "**UK Addendum**") supplements the AWS Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf, or other agreement between Customer and AWS governing the processing of Customer Data (the "**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 DPA.

1. **Applicability.** Except as otherwise set out in this UK Addendum, the terms of the DPA will apply to Customer's use of the Services to process UK Customer Data, and all references to (i) "GDPR" will be replaced with "UK GDPR", (ii) "Customer Data" will be replaced with "UK Customer Data",
(iii) "Standard Contractual Clauses" will be replaced with "UK Standard Contractual Clauses", (iv) "Controller-to-Processor Clauses" will be replaced with "UK Controller-to-Processor Clauses", and
(v) "Processor-to-Processor Clauses" will be replaced with "UK Processor-to-Processor 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 DPA will not apply, and the following Sections will apply:

"**12.2 Application of UK Standard Contractual Clauses.** Subject to Section 12.3, the UK 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**").

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

12.2.2 When Customer is acting as a processor, the UK Processor-to-Processor Clauses will apply to a UK 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 UK Processor-to-Processor Clauses.

12.3 **Alternative Transfer Mechanism.** The UK Standard Contractual Clauses will not apply to a UK Data Transfer if AWS has adopted Binding Corporate Rules (as defined in the UK GDPR) for Processors or 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:

""**International Data Transfer Addendum**" means the international data transfer addendum to the Standard Contractual Clauses issued by the Information

Commissioner's Office under section 119A of the Data Protection Act 2018 on 2 February 2022, and located in Annex A of this UK Addendum.

"**UK Controller-to-Processor Clauses**" means the Controller-to-Processor Clauses, as amended by the International Data Transfer Addendum.

"**UK Processor-to-Processor Clauses**" means the Processor-to-Processor Clauses, as amended by the International Data Transfer Addendum.

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

"**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 "applied GDPR" as defined in section 3 of the Data Protection Act 2018.

"**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. **International Data Transfer Addendum.** Annex A ("International Data Transfer Addendum to the Standard Contractual Clauses") of this UK Addendum will apply in accordance with Section 2 of this UK Addendum.

5. **Entire Agreement; Conflict.** Except as supplemented by this UK Addendum, the DPA (if applicable) and the Agreement will remain in full force and effect. Where both this UK Addendum and the DPA apply to a processing activity, both will apply concurrently. This UK Addendum, together with the 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 A - **International Data Transfer Addendum to the Standard Contractual Clauses (the “Addendum”)**

This Addendum is attached to and forms part of the UK Addendum. The parties hereby enter into this Addendum as a legally binding contract for the purpose of making UK Data Transfers. Unless otherwise defined in this Addendum, all capitalised terms used in this Addendum will have the meanings given to them in the UK Addendum.

Part 1: Tables

Table 1:Parties

Start date	The date that Customer starts to use the Services to transfer UK Customer Data to UK Third Countries.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties’ details	Full legal name: The entity identified as “Customer” in the DPA. Trading name (if different): If different, the trading name for Customer associated with its AWS account or as otherwise specified in the DPA or the Agreement. Main address (if a company registered address): The address for Customer associated with its AWS account or as otherwise specified in the DPA or the Agreement. Official registration number (if any) (company number or similar identifier): If any, the official registration number for Customer associated with its AWS account or as otherwise specified in the DPA or the Agreement.	Full legal name: "AWS” as identified in the DPA. Trading name (if different): N/A Main address (if a company registered address): The address for AWS specified in the Agreement. Official registration number (if any) (company number or similar identifier): If any, the official registration number for AWS specified in the Agreement.

Key Contact	Job Title: The job title for the contact associated with Customer's AWS account, or as otherwise specified in the DPA or the Agreement. Contact details including email: The contact details associated with Customer's AWS account, or as otherwise specified in the DPA or the Agreement.	Job Title: The job title for the contact for AWS specified in the DPA or the Agreement. Contact details including email: The contact details for AWS specified in the DPA or the Agreement.
Signature (if required for the purposes of Section 2)	By using the Services to transfer UK Customer Data to UK Third Countries, the Exporter will be deemed to have signed this Addendum.	By transferring UK Customer Data to UK Third Countries on Customer's instructions, the Importer will be deemed to have signed this Addendum.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The date that Customer starts to use the Services to transfer Customer Data to Third Countries. Reference (if any): N/A Other identifier (if any): This Addendum is appended by reference to the following versions of the Approved EU SCCs (as applicable): • the Controller-to-Processor Clauses available at https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf ; and • the Processor-to-Processor Clauses available at https://d1.awsstatic.com/Processor_to_Processor_SCCs .pdf.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Data exporter(s):

Name: The entity identified as “Customer” in the DPA.

Address: The address for Customer associated with its AWS account or as otherwise specified in
the DPA or the Agreement.

Contact person’s name, position and contact details: The contact details associated with Customer’s AWS account, or as otherwise specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section
1.3 of the DPA.

Signature and date: By using the Services to transfer Customer Data to Third Countries, the data exporter will be deemed to have signed Annex I.

Role (controller / processor): (I) where the Controller-to-Processor Clauses apply, the data exporter will be a controller; and (ii) where the Processor-to-Processor Clauses apply, the data exporter will be a processor.

Data importer(s):

Name: "AWS” as identified in the DPA.

Address: The address for AWS specified in the Agreement.

Contact person’s name, position and contact details: The contact details for AWS specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section
1.3 of the DPA.

Signature and date: By transferring Customer Data to Third Countries on Customer’s instructions, the data importer will be deemed to have signed Annex I.

Role (controller / processor): Processor.

Annex 1B: Description of Transfer:

Categories of data subjects whose personal data is transferred Categories of data subjects are specified in Section 1.3 of the DPA. ***Categories of personal data transferred***

The personal data is described in Section 1.3 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data exporter might include sensitive personal data in the personal data described in Section 1.3 of the DPA.

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

Personal data is transferred in accordance with Customer’s instructions as described in Section 12 of the DPA.

Nature of the processing

The nature of the processing is described in Section 1.3 of the DPA.

Purpose(s) of the data transfer and further processing

To provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Not applicable because the data exporter determines the duration of processing in accordance with the terms of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the processing are described in Section 1.3 of the DPA.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons

The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests, are described in the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The technical and organisational measures that the data importer will impose on sub-processors are described in the DPA.

Annex III: List of Sub processors (Modules 2 and 3 only):

A link to a list of Sub-processors is set out in Section 6 of the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this

Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

       > "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

       > "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex

I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Appendix 4 – Supplementary Addendum to AWS GDPR Data Processing Addendum

The purpose of this supplementary addendum (this "**Addendum**") is to outline supplemental measures that AWS takes to protect Customer Data. This Addendum supplements, but does not modify, the AWS Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf, or other agreement between Customer and AWS governing the processing of Customer Data (the "**DPA**"). Unless otherwise defined in this Addendum, all capitalized terms used in this Addendum will have the meanings given to them in the 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 Addendum restricts Customer's data subjects from exercising their rights under Applicable Data Protection Law. This includes, if applicable, a data subject's 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 Addendum and the 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 Addendum and the 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 Addendum, the DPA and the Agreement will remain in full force and effect. This Addendum, together with the 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. If there is a conflict between the DPA and this Addendum, the terms of this Addendum will control.

Appendix 5 – Standard Contractual Clauses Controller-to Processor Transfers

This attachment is attached to and forms part of the AWS Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf, or other agreement between Customer and AWS governing the processing of Customer Data (the "**DPA**"). Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex
I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the Standard Contractual Clauses included in Decision 2021/915.or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub- processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[2] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third -party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clause

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[3];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time- frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector

and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Grand Duchy of Luxembourg.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the district of Luxembourg City.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as “Customer” in the DPA.

Address: The address for Customer associated with its AWS account or as otherwise specified in the DPA or the Agreement.

Contact person’s name, position and contact details: The contact details associated with Customer’s
account, or as otherwise specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.3 of the DPA.

Signature and date: By using the AWS services to transfer Customer Data to Third Countries, the data exporter will be deemed to have signed this Annex I.

Role (controller / processor): Controller

Data importer(s):

Name: "AWS” as identified in the DPA.

Address: The address for AWS specified in the Agreement.

Contact person’s name, position and contact details: The contact details for AWS specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.3 of the DPA.

Signature and date: By transferring Customer Data to Third Countries on Customer’s instructions, the
data importer will be deemed to have signed this Annex I.

Role (controller / processor): Processor

B. B DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred Categories of data subjects are specified in Section 1.3 of the DPA. ***Categories of personal data transferred***

The personal data is described in Section 1.3 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into **consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**

The data exporter might include sensitive personal data in the personal data described in Section 1.3 of the DPA.

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

Personal data is transferred in accordance with Customer's instructions as described in Section 12 of the DPA.

Nature of the processing

The nature of the processing is described in Section 1.3 of the DPA.

Purpose(s) of the data transfer and further processing

To provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Not applicable because the data exporter determines the duration of processing in accordance with the terms of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the processing are described in Section 1.3 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) **(including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons**

The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests, are described in the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to **be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.**

The technical and organisational measures that the data importer will impose on sub-processors are described in the DPA.

ANNEX III

ADDITIONAL CLAUSES

The Limitations of Liability section of the Agreement (usually Section 9 of the Agreement) is an additional clause pursuant to Clause 2 of these Clauses.

Appendix 6 – Standard Contractual Clauses Processor-to Processor Transfers

This attachment is attached to and forms part of the AWS Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf, or other agreement between Customer and AWS governing the processing of Customer Data (the "**DPA**"). Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the Standard Contractual Clauses included in Decision 2021/915.standard contractual clauses laid down in these Clauses in a wider contract and/or to add other Clauses or additional safeguards provided that they do not contradict, directly or indirectly, these clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[2].

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the

[2] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the controller's general authorisation for the engagement of sub- processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third -party beneficiary rights for data subjects.[4] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third -party beneficiary clause with the sub-processor whereby

- in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[4] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub- processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(e) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(f) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clause

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these

Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for

disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time- frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or the supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two

Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Grand Duchy of Luxembourg.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the district of Luxembourg City.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as “Customer” in the DPA.

Address: The address for Customer associated with its AWS account or as otherwise specified in the DPA or the Agreement.

Contact person’s name, position and contact details: The contact details associated with Customer’s
account, or as otherwise specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.3 of the DPA.

Signature and date: By using the Services to transfer Customer Data to Third Countries, the data exporter will be deemed to have signed this Annex I.

Role (controller / processor): Processor

Data importer(s):

Name: "AWS” as identified in the DPA.
Address: The address for AWS specified in the DPA or the Agreement.

Contact person’s name, position and contact details: The contact details for AWS specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.3 of the DPA.
Signature and date: By transferring Customer Data to Third Countries on Customer’s instructions, the
data importer will be deemed to have signed this Annex I.

Role (controller / processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred Categories of data subjects are described in Section 1.3 of the DPA. ***Categories of personal data transferred***

The personal data is described in Section 1.3 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into **consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**

The data exporter might include sensitive personal data in the personal data described in Section 1.3 of the DPA.

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

Personal data is transferred in accordance with Customer's instructions as described in Section 12 of the DPA

Nature of the processing

The nature of the processing is described in Section 1.3 of the DPA.

Purpose(s) of the data transfer and further processing

To provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data exporter determines the duration of processing in accordance with the terms of the DPA. ***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*** The subject matter, nature and duration of the processing are described in Section 1.3 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

***Description of the technical and organisational measures implemented by the data importer(s)* (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons**

The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests are described in the DPA.

***For transfers to (sub-) processors, also describe the specific technical and organisational measures to be* taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter**

The technical and organisational measures that the data importer will impose on sub-processors are described in the DPA.

ANNEX III

ADDITIONAL CLAUSES

The Limitations of Liability section of the Agreement (usually Section 9 of the Agreement) is an additional clause pursuant to Clause 2 of these Clauses.