AWS DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is made and entered into by and between Amazon Web Services, Inc., a Delaware corporation ("**AWS**") and the customer specified in the table below ("**Customer**").

AMAZON WEB SERVICES, INC. **By:** DocuSigned by: Rachel Thornton **Name:** Rachel Thornton **Title:** Vice President, Field and Partner Marketing **Signature Date:** December 14, 2016 **Address:** **410 Terry Avenue North** **Seattle, WA 98109-5210** **Attention: General Counsel**	**Customer Name (Required):** Promidata BV (full legal entity name) **By (Signature Required):** **Your Printed Name (Required):** E. Bakker **Your Title (Optional):** **Signature Date (Required):** 30 sept. 2020 **Customer Address (Required):** Hoofdstraat 81 6461 CN Kerkrade, The Netherlands **Attention:**

This Addendum includes the Data Processing Terms and the attached Annexes 1-2 and supplements the AWS Customer Agreement available at http://aws.amazon.com/agreement, (as updated from time to time) between Customer and AWS, or other agreement between Customer and AWS governing Customer's use of the Service Offerings (the "**Agreement**"). This Addendum will be effective as of the day AWS receives a complete and executed Addendum from Customer in accordance with the instructions under paragraphs 1 and 2 below (the "**Addendum Effective Date**").

1. **Instructions.** This Addendum (including the Standard Contractual Clauses, as defined below) has been pre-signed on behalf of AWS. To enter into this Addendum, Customer must:
   a. Complete the table above by signing and providing the customer full legal entity name, address and signatory information; and
   b. Submit the completed and signed Addendum to AWS via email to aws-dpa-submissions@amazon.com.
2. **Effectiveness.**
   a. This Addendum will be effective only if it is executed and submitted to AWS in accordance with paragraph 1 above and this paragraph 2, and all items identified as "Required" in the table are completed accurately and in full. If Customer makes any deletions or other revisions to this Addendum, then this Addendum will be null and void. This Addendum will only apply to Customer's use of AWS accounts (including any use by agents or subcontractors (including any of its affiliates who are acting as an agent or subcontractor of Customer) performing work on behalf of Customer) that include the Customer's full legal entity name (matching the one provided in the table above) in the "Company Name" field associated with the AWS account. If Customer has affiliates with their own AWS accounts that need coverage under an AWS Data Processing Addendum, in order to have coverage each affiliate must sign its own AWS Data Processing Addendum with AWS, in which case, the full legal entity name entered in the "Company Name" field associated with the AWS account will be the name of the affiliate.
   b. This Addendum applies only to AWS Service Offerings purchased from AWS and does not apply to AWS Service Offerings Customer purchases from any seller of record other than AWS including AWS value-added resellers.
   c. Customer signatory represents to AWS that he or she has the legal authority to bind Customer and is lawfully able to enter into contracts (e.g., is not a minor).
   d. This Addendum will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of this Addendum.

Data Processing Terms

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

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

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

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

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and any replacement directive or regulation imposing equivalent obligations.

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

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

"**Standard Contractual Clauses**" means Annex 2 attached to and forming part of this Addendum pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive.

2. Data Processing.

2.1 **Scope and Roles.** This Addendum applies when Customer Data is processed by AWS. In this context, Customer may act as "controller" or "processor" and AWS may act as "processor" or "sub-processor" with respect to Customer Data (as each term is defined in the Directive).

2.2 **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 Addendum, including all statutory requirements relating to data protection.

2.3 **Instructions for Data Processing.** AWS will process Customer Data in accordance with Customer's instructions. The parties agree that this Addendum is Customer's complete and final instructions to AWS in relation to processing of Customer Data. Processing outside the scope of this Addendum (if any) will require prior written agreement between AWS and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to AWS for carrying out such instructions. Customer may terminate this Addendum if AWS declines to follow instructions requested by Customer that are outside the scope of this Addendum.

2.4 **Access or Use.** AWS will not access or use Customer Data, except as necessary to provide the Service Offerings initiated by Customer.

2.5 **Disclosure.** AWS will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends AWS a demand for Customer Data, AWS will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, 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.

2.6 **AWS Personnel.** AWS restricts its personnel from processing Customer Data without authorisation by AWS as described in the AWS Security Standards. AWS will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

2.7 **Customer Controls.** The Service Offerings provide Customer with controls to enable Customer to retrieve, correct, delete, or block Customer Data as described in the Documentation. AWS makes available a number of security features and functionalities that Customer may elect to use. Customer is responsible for properly (a) configuring the Service Offerings, (b) using the controls available in connection with the Service Offerings (including the security controls), and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, deletion and backup of Customer Data, which may include use of encryption technology to protect Customer Data from unauthorized access and routine archiving of Customer Data.

2.8 **Transfers of Personal Data.**

2.8.1 **Regions.** Customer may specify the AWS region(s) where Customer Data will be processed within the AWS Network, including the EU (Dublin) Region, the EU (Frankfurt) Region and the EU (London) Region (each a "**Region**"). Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order) as described in Section 2.5.

2.8.2 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Directive). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply: (a) if AWS is acting as a sub-processor (as defined in the Standard Contractual Clauses) with respect to Customer Data, or (b) if AWS has adopted Binding Corporate Rules or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the Directive) outside the EEA.

3. Security Responsibilities of AWS

3.1 AWS is responsible for implementing and maintaining the technical and organisational measures for the AWS Network as described in the AWS Security Standards and this Section of this Addendum designed to help Customer secure Customer Data against unauthorized processing and accidental or unlawful loss, access or disclosure.

3.2 The technical and organisational measures include the following:

(i) AWS has implemented and will maintain measures to maintain the physical security of the Facilities as set out in Section 1.2 of the AWS Security Standards;

(ii) AWS has implemented and will maintain measures to maintain the security of the AWS Network as set out in Section 1.1 of the AWS Security Standards;

(iii) AWS has implemented and will maintain measures to control access rights for AWS employees and contractors in relation to the AWS Network as set out in Section 1.1 of the AWS Security Standards. Customer has implemented and will maintain measures to control access rights to Customer Data; and

(iv) AWS will process Customer Data in accordance with Customer's instructions as described in Section 2.3 of this Addendum.

4. Certifications.

4.1 As of the Addendum Effective Date, AWS is certified under ISO 27001 and agrees to maintain an information security program for the Services that complies with the ISO 27001 standards or such other alternative standards as are substantially equivalent to ISO 27001 for the establishment, implementation, control, and improvement of the AWS Security Standards.

4.2 Customer is solely responsible for reviewing the information made available by AWS relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.

5. Audit of Technical and Organisational Measures.

5.1 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. If Customer's Agreement does not include a provision protecting AWS Confidential Information, then Reports will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering the Report (an "**NDA**").

5.2 At Customer's written request, AWS will provide Customer with a confidential Report so that Customer can reasonably verify AWS's compliance with the security obligations under this Addendum. The Summary Report will constitute AWS's Confidential Information under the confidentiality provisions of the Agreement or the NDA, as applicable.

5.3 If the Standard Contractual Clauses apply, then Customer agrees to exercise its audit right by instructing AWS to execute the audit as described in this Section of the Addendum. If Customer has not opted out of the Standard Contractual Clauses and desires to change this instruction regarding exercising this audit right, then Customer has the right to change this instruction, as mentioned in the Standard Contractual Clauses, which shall be requested in writing. If the Standard Contractual Clauses apply, then nothing in this Section of the Addendum varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

6. Security Breach Notification.

6.1 If AWS becomes aware of either (a) any unlawful access to any Customer Data stored on AWS's equipment or in AWS's facilities; or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of Customer Data (each a "**Security Incident**"), AWS will promptly: (a) notify Customer of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

6.2 Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section. 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 may 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 IP addresses or headers) or similar incidents; and

(ii) AWS's obligation to report or respond to a Security Incident under this Section 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.

6.3 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 at all times.

7. Subcontracting.

7.1 **Authorised Subcontractors.** Customer agrees that AWS may use subcontractors to fulfil its contractual obligations under this Addendum or to provide certain services on its behalf, such as providing support services. The AWS website lists subcontractors that are currently authorized by AWS to access Customer Data. At least 30 days before AWS authorizes and permits any new subcontractor to access Customer Data, AWS will update the applicable website. If Customer does not approve of a new subcontractor, then without prejudice to any termination rights Customer has under the Agreement and subject to the applicable terms and conditions, Customer may move the Customer Data to another AWS Region where the new subcontractor who is not approved by Customer is not an authorized subcontractor. Customer hereby consents to AWS's use of subcontractors as described in this Section 7. Except as set forth in this Section 7, or as Customer may otherwise authorize, AWS will not permit any subcontractor to access Customer Data.

7.2 **Subcontractor Obligations.** Where AWS authorises any subcontractor as described in this Section 7:

(i) AWS will restrict the subcontractor's access to Customer Data only to what is necessary to maintain the Service Offerings or to provide the Service Offerings to Customer and any End Users in accordance with the Documentation and AWS will prohibit the subcontractor from accessing Customer Data for any other purpose;

(ii) AWS will impose appropriate contractual obligations in writing upon the subcontractor that are no less protective than this Addendum, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights; and

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

8. 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 (e.g. 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.

9. Nondisclosure. Customer agrees that the details of this Addendum are not publicly known and constitute AWS's Confidential Information under the confidentiality provisions of the Agreement or NDA. If the Agreement does not include a confidentiality provision protecting AWS Confidential Information and Customer and AWS or its affiliates do not have an NDA in place covering this Addendum, then Customer will not disclose the contents of this Addendum to any third party except as required by law.

10. Entire Agreement; Conflict. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

[Remainder of Page Intentionally Left Blank]

Annex 1

AWS Security Standards

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

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

   1.2 **Physical Security**

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

      1.2.2 **Limited Employee and Contractor Access.** AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

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

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

[Remainder of Page Intentionally Left Blank]

Annex 2

Standard Contractual Clauses (processors)

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

The entity identified as "Customer" in the Addendum
(the "**data exporter**")

and

Amazon Web Services Inc.

410 Terry Avenue North, Seattle, WA 98109-5210, USA.

(the "**data importer"**)

each a "party"; together "the parties",

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

***Obligations of the data importer*[1]**

The data importer agrees and warrants:

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

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the

data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

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

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity identified as "Customer" in the Addendum

Data importer

The data importer is Amazon Web Services, Inc., a provider of web services.

Data subjects

Data subjects include the data exporter's customers and end-users.

Categories of data

The personal data relating to individuals which is uploaded onto the AWS Services by the data exporter.

Processing operations

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

Compute, Storage and Content Delivery on the AWS Network

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the signature page on page 1 of this Addendum, the parties will be deemed to have signed this Appendix 2.

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

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