the foregoing, if Customer reasonably believes that an audit is necessary to meet its obligations under any applicable Data Protection Laws, Customer may request that a third-party (at Customer's expense) conduct an audit and Rh will work with Customer to the extent feasible to accommodate Customer's request. If Rh is unable to accommodate Customer's request, Customer is entitled to terminate this DPA and the Agreement. Where the Model Clauses apply, nothing in this Section 6.3 varies or modifies the Model Clauses nor affects any supervisory authority's or data subject's rights under the Model Clauses.

7. Transfers of Personal Data

7.1. Data center locations: Rh may transfer and process Customer Data anywhere in the world where Rh its Affiliates or its Subprocessors maintain data processing operations. Rh shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

7.2. Application of Model Clauses: To the extent that Jask processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the European Economic Area (including the United Kingdom) ("EEA") or Switzerland, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Jask shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by complying with the Model Clauses. Rh agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that Customer may be an entity located outside of the EEA).

7.3. Alternative Data Export Solutions: Notwithstanding the foregoing Section 7.2, the parties agree that in the event Rh adopts Binding Corporate Rules or another alternative data export solution (as recognized under EU Data Protection Laws), then the Model Clauses will cease to apply with effect from the date that Rh implements such new data export solution.

8. Data Storage and Return or Deletion of Data

8.1. Data Storage. Area 1 will abide by the following with respect to storage of Customer Data:

8.1.1. Area 1 will not store or retain any Customer Data except as necessary to perform the Services under the Agreement.

8.1.2. Area 1 will (i) inform Customer of all countries where Customer Data is Processed or stored and (ii) obtain consent from Customer for Processing or storage in the identified countries. As of the Effective Date, Area 1 stores Customer Data in the following countries: United States, United Kingdom, Ireland and Germany.

8.2. Data Deletion. Within thirty (30) calendar days of the Agreement's expiration or termination, or sooner if requested by Customer, Area 1 will securely destroy (per subsection (iii) below) all copies of Customer Data (including automatically created archival copies), except to the extent Rh is required by applicable law to retain some or all of the Customer Data (in which case, Rh shall implement reasonable measures to isolate the Customer Data from any further processing).

9. Cooperation

9.1. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Rh shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to Rh shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Rh is required to respond to such a request, Rh will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

9.2. If a law enforcement agency sends Rh a demand for Customer Data (for example, through a subpoena or court order), Rh will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Rh may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Rh will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Rh is legally prohibited from doing so.

9.3. To the extent Jask is required under EU Data Protection Laws, Jask will (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

10. General

10.1. For the avoidance of doubt, any claim or remedies the Customer may have against Jask, any of its Affiliates and their respective employees, agents and subprocessors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) under EU Data Protection Laws, including any claims relating to damages paid to a data subject; and (iv) breach of its obligations under the Model Clauses, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Customer further agrees that any regulatory penalties incurred by Jask in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Area 1 Security's liability under the Agreement as if it were liability to the Customer under the Agreement. Nothing in this DPA is intended to limit the Parties' direct liability towards data subjects or applicable supervisory data protection authorities.

10.2. Any claims against Jask or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10.3. No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

10.4. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

10.5. In the event of any conflict between this DPA and any privacy-related provisions set out in the Agreement or any other existing data protection terms agreed to between the parties, the terms of this DPA shall prevail.

10.6. This DPA is provided in a pre-printed, pre-signed and read-only electronic form published by Jask. Any modification of the provisions or terms of this DPA will be considered to make the pre-signatures below null and void. In the event that this DPA contains modifications, even if signed by the representatives of Jask other than an authorised signatory, such modifications shall be null and void and this DPA shall be construed as if such modifications had not been made

DATA PROTECTION ADDENDUM IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

Jask, Labs Inc.: By:	Customer:
Name: **Blake Darche**	By:
	Name:
Title: **CSO & Chief Privacy Officer**	Title:
Date: **05/25/2018**	Date:

Annex A

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES TO BE IMPLEMENTED BY AREA 1 SECURITY

Area 1 Security provides Annex A to customers under a valid Agreement and to prospective customers under a non-disclosure agreement. Please email privacy@jask.com for a copy.

Security Measures shall include:

i) Pseudonymisation of Customer Data where appropriate, and encryption of Customer Data in transit and at rest;

ii) The ability to ensure the ongoing confidentiality, integrity, availability of Area 1 Security's Processing and Customer Data;

iii) The ability to restore the availability and access to Customer Data in the event of a physical or technical incident;

iv) A process for regularly testing, assessing and evaluating of the effectiveness of the Area 1 Security's Information Security Program to ensure the security of Customer Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

Annex B
Model Clauses

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

Name of the data exporting organisation:

The identity identified as the "data exporter" in Appendix 1 of these Contractual Clauses

(the data exporter)

And

Name of the data importing organisation:
Jask Labs, Inc.,
Address: 11501 Rock Rose Ave Suite 200 Austin, TX 78758
Tel: (800) 335-1637
Email: privacy@area 1security.com

(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.

1. Definitions

For the purposes of the Clauses:

'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;

'the data exporter' means the controller who transfers the personal data;

'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;

'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;

'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;

'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

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.

3. Third-party beneficiary clause
   - 3.1. 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.
   - 3.2. 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.
   - 3.3. 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.
   - 3.4. 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.

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).

5. Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

(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.

6. Liability
   6.1. 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.
   6.2. 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.
   6.3. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
   6.4. 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.

7. Mediation and jurisdiction
   7.1. 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.
   7.2. 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.

8. Cooperation with supervisory authorities
   8.1. 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.
   8.2. 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.
   8.3. 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).

9. Governing Law

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

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.

11. Subprocessing
    11.1. 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.
    11.2. 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.
    11.3. 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.
    11.4. 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.

12. Obligation after the termination of personal data processing services
    12.1. 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.
    12.2. 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

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter / Description of Customer

The data exporter is (please specify briefly activities relevant to the transfer):

The data exporter is: (i) the legal entity that is identified as "Customer" and who has executed these Standard Contractual Clauses, and, (ii) all members of the Customers Group (as defined in the data processing agreement between the data exporter and data importer) established within the European Economic Area (including United Kingdom) (EEA) and Switzerland that have purchased a subscription for the data importers services as set forth in the underlying agreement for services between the data exporter and the data importer (the "Agreement')

Data importer / Nature of Services provided by Jask

The data importer is (please specify briefly your activities relevant to the transfer):

Jask Labs, Inc. provides cloud-based security solutions to help businesses protect against phishing attacks which involves processing Personal Data provided by, and pursuant to the instructions and directions of Customer, in accordance with the terms of the Agreement ("Services").

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- *Prospects, customers, business partners and vendors of data exporter (who are natural persons)*
- *Employees or contact persons of data exporter's prospects, customers, business partners and vendors.*
- *Employees, agents, advisors, freelancers of data exporter (who are natural persons)*

Categories of data

The personal data transferred concern the following categories of data (please specify):
Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by Data Exporter in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

- *Identification and contact data (name, address, title, contact details),*
- *Financial information (credit card details, account details, payment information)*
- *Employment details (employer, job title, geographic location, area of responsibility)*
- *IT information (IP addresses, usage data, cookies data, device specific information, connection data, location data)*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The Services are not designed to require the submission of special categories of Personal Data. Therefore, it is not anticipated that data exporter will submit special categories of Personal Data to the Services, and to the extent such data is submitted to the Services, it is determined and controlled by data exporter in its sole discretion.

Nature of Processing operations

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

The objective of Processing of Personal Data by Jask is the performance of the Services pursuant to the Agreement.

Duration of Processing Operations:

The term of the Agreement.

Appendix 2 to the Standard Contractual Clauses

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

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

The security measures are described in Annex A of the Data Protection Addendum.

Appendix 3 to the Standard Contractual Clauses

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

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's confidential information as such term is defined in the Agreement (defined in Appendix 1) and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions in accordance with and as described in Section 3.3 of the Data Protection Addendum incorporating these Clauses (the "DPA")
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance (“Cure Period”).
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described Section 6 (Audit Reports) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with Section 4 (Subprocessing) of the DPA.

DATA EXPORTER

Name:.....

Authorised Signature .....

DATA IMPORTER

Name:. **Jask**

Authorised Signature .....

Damian Miller, CSO & Chief Privacy Officer

Sub-Processors

striekSub-Processor	Activity
Amazon Web Services	Website, Area 1 Horizon Product
Google	Area 1 Horizon Data Warehouse
Salesforce	Sales Account Records
ZenDesk	Support Tickets