INTEGRAL AD SCIENCE, INC.
DATA PROTECTION TERMS

The following data protection terms and conditions (the "**Data Protection Terms**"), including all appended Schedules and Annexes, form an integral part of the underlying Agreement (the "Agreement"). These Data Protection Terms govern the responsibilities of the Parties with respect to the processing of Customer Personal Data in the course of Customer's use of the Services. The Parties agree that these Data Protection Terms replace or supersede any existing Data Protection Terms or similar documents that the Parties may have previously entered into with regard to the Services. In the event of any conflict or inconsistency between the Agreement and these Data Protection Terms and any Schedules or Annexes hereto, the Data Protection Terms and/or any applicable Schedule or Annex shall govern.

1. Roles of the Parties.

(a) Customer shall be a Controller of Customer Personal Data.

(b) Customer and IAS shall both be Controllers of IP addresses generated through Customer's use of the Services that IAS uses for purposes of detecting ad fraud.

(c) IAS shall be the Processor of Customer Personal Data not covered by 1(b) above processed in the course of Customer's use of the Services.

2. Definitions.

All undefined capitalized Terms herein shall have the same meaning as in the Agreement, as applicable. In the event of any conflict or inconsistency between the Agreement and these Data Protection Terms and any Annexes hereto, as applicable, the Data Protection Terms and Annexes shall govern with respect to the personal data addressed in each applicable Annex.

In these Data Protection Terms:

(a) "**Applicable Data Protection Laws**" means collectively all applicable laws and regulations, as revised from time to time, related to data protection and privacy that apply to the Parties with regard to the processing of Customer Personal Data. The term, "**U.S. Federal and State Privacy Laws**," shall refer to a subset of Applicable Data Protection Laws applicable in the United States, including the California Consumer Privacy Act as amended by the California Privacy Rights Act of 2020.

(b) "**Controller**" means the business, organization, operator, or other natural or legal person that, alone or jointly with others, determines the purposes and means of Personal Data processing.

(c) "**Customer Personal Data**" means Personal Data processed by IAS on behalf of Customer in connection with the Services, including a subset of Ad Performance data limited to IP Addresses.

(d) "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates.

(e) "**Emergency Replacement**" means the sudden replacement of a Sub-Processor where such change is outside of IAS's reasonable control (such as if the Sub-Processor ceases business, abruptly discontinues its services to IAS, or breaches its contractual duties owed to IAS).

(f) "**Personal Data**" means any information relating directly or indirectly to an identified or identifiable natural person. "Personal Data" also includes "personal information" and similar concepts relating to a legal person to the extent such information is protected under Applicable Data Protection Laws.

(g) "**Processing**" (and the related terms "process," "processes," and "processed") means any operation or set of operations performed upon Personal Data, including access, alteration, collection, combination, destruction, disclosure, dissemination, erasure, organization, retrieval, storage, structuring, transfer, and use.

(h) "**Processor**" means the service provider, data processor, vendor, or other natural or legal person engaged to process Personal Data on behalf of the Controller.

(i) "**Sub-Processor**" means a Processor engaged by IAS to process Personal Data for and on behalf of Customer.

(j) "**Regulator**" means any competent supervisory authority under Applicable Data Protection Law.

3. General Obligations.

(a) **Applicability of these Data Protection Terms**. These Data Protection Terms apply only when, and to the extent that, IAS processes Customer Personal Data subject to Applicable Data Protection Laws in the context of the Services.

(b) Customer shall:

(i) ensure that all necessary consents (if any) are obtained and all necessary notices and/or consent withdrawal mechanisms (if any) are provided (whether by applicable publishers, industry initiatives, Customer, or otherwise) so as to enable IAS to obtain and process Customer Personal Data lawfully in accordance with Applicable Data Protection Laws in providing the Services;

(ii) ensure that content (if any) containing IAS tags or pixels displays a link to appropriate privacy notice that explains the processing described in the Agreement, including any transfer of Customer Personal Data to IAS, in a manner which complies with Applicable Data Protection Laws. IAS will provide Customer with such information as the Customer may reasonably request in order to comply with this obligation.

(iii) ensure that Customer relies on a valid legal basis for processing, including Customer Personal Data with IAS, when required by Applicable Data Protection Laws.

(c) Each Party shall:

(i) comply with its obligations under Applicable Data Protection Laws and shall not take any action or make any omission which might be reasonably likely to put the other Party in breach of Applicable Data Protection Laws.

(ii) put in place industry-standard technical and organizational measures to ensure a level of security for Personal Data appropriate to the risks of the processing, including to protect against unauthorized or unlawful processing and accidental loss, destruction, or damage. IAS shall ensure that at least those measures identified in **Annex II of Schedule 2** are maintained.

(iii) when required by Applicable Data Protection Laws, timely notify the other Party after becoming aware of a security breach, unauthorized access, misappropriation, loss, damage, or other compromise of the security, confidentiality, or integrity of Customer Personal Data ("**Security Breach**") in which case the other Party that has suffered the Security Breach shall provide reasonable assistance in relation to remediating the Security Breach and complying with related obligations under Applicable Data Protection Laws.

(iv) when required by Applicable Data Protection Laws, provide reasonable assistance to the other Party in the event of any complaint, request, or communication from a Regulator or Data Subject alleging non-compliance with Applicable Data Protection Laws or these Data Protection Terms as a result of the processing carried out under this Agreement.

(v) when required by Applicable Data Protection Laws, provide reasonable assistance requested by the other Party in relation to compliance with any obligations under Applicable Data Protection Laws, including providing any additional disclosures and enabling any additional Data Subject controls that the Parties agree are necessary pursuant to Applicable Data Protection Laws for the setting, processing, or collection of Customer Personal Data (through IAS tags or pixels). No Party will unreasonably withhold or delay its agreement to any proposal in this regard.

(vi) agree and warrant to work together in good faith to amend these Data Protection Terms to address compliance with any new, updated, or otherwise amended Applicable Data Protection Laws.

4. Obligations where IAS acts as a Controller. Where IAS acts as a Controller under Applicable Data Protection Laws:

(a) IAS shall remain a service provider or processor under applicable U.S. Federal and State Privacy Law.

(b) Customer will provide IAS with such information and cooperation as IAS may reasonably request to assist IAS in complying (and evidencing its compliance) with Applicable Data Protection Laws in relation to the provision of information about IAS's processing to Data Subjects.

(c) if IAS uses Customer Personal Data, IAS shall use all reasonable endeavors to keep such Customer Personal Data up to date and accurate.

5. Obligations on IAS where IAS acts as a Processor. Where IAS acts as a Processor, IAS warrants that it shall when required by Applicable Data Protection Laws:

(a) Process Customer Personal Data only on Customer's instructions, as documented in the Agreement and any applicable Schedules or Annexes to these Data Protection Terms, or as otherwise provided in writing by the Customer.

(b) ensure that all individuals authorized to process Personal Data are subject to binding obligation to keep that Personal Data confidential.

(c) provide Customer with reasonable assistance in relation to Customer's obligations under Applicable Data Protection Laws, including in relation to responding to requests from Data Subjects to exercise privacy rights, carrying out data protection impact assessments or similar privacy assessments, and consulting with Regulators

(d) delete or take any other action at Customer's request, to the extent possible, with respect to Customer Personal Data maintained by IAS, and notify relevant Sub-Processors to take corresponding actions, unless Customer's requested action is impossible or involves disproportionate effort. If processing a request is impossible or requires disproportionate effort, IAS will provide Customer with a written explanation describing the impossibility of the request or disproportionate effort required.

(e) not sell, retain, use, or disclose Customer Personal Data for any purpose other than to provide the Services.

(f) engage Sub-Processor in accordance with the following provisions:

(i) IAS may use its own affiliates as Sub-Processors to provide the Services.

(ii) with the exception of Emergency Replacements, only engage additional Sub-Processors where such engagement is notified to Customer prior to such engagement.

(iii) if Customer reasonably objects to any new Sub-Processors(s), Customer can do so within fifteen (15) calendar days of receiving notice of the new Sub-Processor by following the instructions set out in such notice.

(iv) if Customer does not object during such time period, the new Sub-Processor(s) shall be deemed to be agreed upon and consented to by Customer.

(v) in the event of such an objection, the Parties shall discuss the objection in good faith and shall take reasonable steps to find a mutually agreeable remedy to Customer's objection, by one of the following options: (1) IAS will abort plans to use the Sub-Processor with regard to Customer Personal Data; (2) IAS will take the corrective steps requested by Customer in its objection (thereby removing Customer's objection) and proceed to use the Sub-Processor to Process Customer's Personal Data; or (3) IAS may cease to provide, or Customer may agree not to use (temporarily or permanently), the particular aspect of the Services that would involve the Sub-Processor's processing of Customer Personal Data. If no such remedy can be found within ninety (90) calendar days after the objection has arisen, any Party shall have the right to terminate any Services that would involve the processing of Customer Personal Data by the objectionable Sub-Processor.

(vi) where an Emergency Replacement is required, IAS will inform Customer of the Emergency Replacement as soon as possible and the process to formally appoint such Sub-Processor defined above shall be triggered.

(vii) all processing by Sub-Processors is subject to a written agreement with Sub-Processors which contains any terms required by Applicable Data Protection Laws, including when applicable that IAS will remain fully liable to Customer for performance of the Sub-Processors engaged.

(g) make available all information reasonably requested by Customer in relation to its processing of Customer Personal Data.

(h) allow for and contribute to audits, including inspections, of IAS systems to solely confirm compliance with these Data Protection Terms or Applicable Data Protection Laws. Customer shall give IAS reasonable prior notice of any such audit or inspection and shall, to the extent allowable by law, be responsible for all reasonable costs incurred by IAS in participating in such an audit, calculated on a time and materials basis.

(i) securely delete all Customer Personal Data processed (and not previously deleted in accordance with IAS standard data deletion schedules) at the termination of the processing described in the Agreement unless Customer requests in writing that Customer Personal Data be returned to Customer.

6. Applicable Data Protection and Jurisdiction-Specific Requirements. Customer acknowledges that Customer Personal Data is processed by IAS, which is located in the United States, and the Processing may include the cross-border transfer of Customer Personal Data. The Parties agree to enter into any jurisdiction-specific Annex(es) as required under Applicable Data Protection Laws in the form of additional Schedules, which shall be incorporated into the Agreement via annexes to these Data Protection Terms.

Schedule 1

CALIFORNIA CONSUMER PRIVACY ACT SUPPLEMENT

The following CCPA data protection supplement (the "**CCPA Supplement**") lays out additional responsibilities of IAS and Customer with respect to the processing of personal information, which is subject to the CCPA, as amended by the California Privacy Rights Act of 2020, that is processed in the course of Customer's use of the Services. All undefined capitalized terms herein shall have the same meaning as the Agreement and/or the Data Protection Terms, as applicable.

For purposes of this CCPA Supplement, the terms "aggregate consumer information," "business," "business purpose," "deidentified information," "personal information," "processing," "sell," "service provider," and "share" shall have the same meaning as in the CCPA.

For clarity, the provisions of this CCPA Supplement do not apply to aggregate consumer information, deidentified information, or any information that is no longer considered personal information, including by application of deidentification or aggregation techniques that meet the requirements of the CCPA.

IAS agrees to comply with the CCPA during the performance of the Agreement and grants Customer the right to take reasonable and appropriate steps to ensure IAS processes personal information the Customer makes available to IAS in compliance with the CCPA. Upon written notice from Customer, IAS will make available to Customer appropriate information reasonably necessary for demonstrating IAS's compliance with its obligations under the CCPA.

IAS will notify Customer if IAS determines that it can no longer meet its obligations under this CCPA Supplement or the CCPA. Upon such notice, Customer may take reasonable and appropriate steps to stop and remediate any unauthorized use of personal information made available by Customer to IAS.

Each Party agrees and warrants it will work together in good faith with the other Party to amend this CCPA Supplement as necessary to address compliance with any new CCPA requirements.

<u>Obligations on IAS where IAS acts as a Service Provider</u>

1. The purpose of personal information processing is for IAS as the service provider to provide the IAS Services to Customer as the business as specified in the Agreement, including:

    a. Performing services on behalf of the business, such as:

        i. Maintaining and servicing Customer accounts,

        ii. Providing customer service;

iii. Processing or fulfilling Customer's orders and other transactions;

iv. Verifying Customer's information; and

v. Providing analytic services to Customer.

b. Providing advertising and marketing services, such as:

i. Providing a platform for advertising inventory management; and

ii. Offering services to optimize advertising performance.

c. Auditing related to counting, verifying, and quality control of ad impressions.

d. Helping to ensure security and integrity, such as:

i. Processing personal information from advertisements placed on or within Customer's webpages, advertisement servers, video players, and/or mobile applications to analyze and detect any advertisement fraud or invalid traffic; and

ii. Processing personal information to ensure Customer's advertisements are not served in irrelevant or inappropriate jurisdictions.

e. Debugging to identify and repair errors that impair intended functionality.

f. Short-term, transient uses.

g. Internal research for technological development.

h. Verification and maintenance of the quality of IAS services.

2. IAS and Customer agree that, as to processing of personal information collected as part of providing the IAS Services as described in the Agreement and the Data Protection Terms, IAS is a service provider and Customer is the business. Accordingly, except as otherwise permitted by the CCPA, IAS shall not:

a. Sell or share the personal information

b. Retain, use, or disclose the personal information for any purpose other than for the business purposes as set forth in Clause 1 of this CCPA Supplement, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the IAS Services.

c. Retain, use, or disclose the personal information outside of the direct business relationship between IAS and Customer.

d. Combine personal information collected pursuant to the Agreement with Customer with personal information received from any other source or collected from IAS's own interaction with a consumer, except as expressly permitted under the CCPA.

Schedule 2

STANDARD CONTRACTUAL

CLAUSES MODULE ONE: CONTROLLER-TO-CONTROLLER

MODULE TWO: CONTROLLER-TO-PROCESSOR

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.

[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, 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.

(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 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 – Module One: Clause 8.5(e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Module Two: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One and Two: 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

(Omitted)

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.

MODULE ONE: Transfer controller to controller

8.1 **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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter ‘personal data breach’). In

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data 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') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer

[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 purpose of these Clauses.

shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

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 ([4]) (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 Regulation of (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

[4] 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 purpose of these Clauses.

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

MODULE TWO: Transfer controller to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION 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 fifteen (15) calendar 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.([5]) 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 the obligations to which the data importer is subject pursuant to these Clauses.

(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.

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

(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

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.([6]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex **I**; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

[6] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer Controller to Processor

(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 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.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(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

MODULE ONE: Transfer controller to controller

(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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

MODULE TWO: Transfer controller to processor

(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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(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 Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(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([7]);

(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).

(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

[7] 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.

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

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 Italy.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(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 Italy.

(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 to Schedule 2

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

A. List of Parties

Data exporter(s):

1. **Name and Address**: The Customer, as set forth in the Underlying Agreement.

Contact person's name, position and contact details: See contact details for data exporter's representative, as set forth in the Underlying Agreement.

Activities relevant to the data transferred under these Clauses: Provide Customer Personal Data to IAS for ad fraud and non-precise geo-verification services.

Signature and date: Signed and dated as of the date of the Underlying Agreement.

Role (controller/processor): Controller

Data Importer(s):

Name and address: Integral Ad Science, Inc., 95 Morton Street, Floor 8, New York, NY 10014

Contact person's name, position and contact details: See contact details for data importer's representative, as set forth in the Underlying Agreement.

Activities relevant to the data transferred under these Clauses: Processing to enable delivery and optimization of Customer's advertisements.

Signature and date: Signed and dated as of the date of the Underlying Agreement.

Role (controller/processor): Controller (for ad fraud services) or processor (for non-precise geo- verification Services).

B. Description of Transfer for Services

Categories of data subjects whose personal data is transferred

Visitors to websites, mobile applications, advertisement servers, video players, or other locations where Customer serves digital advertisements.

Categories of personal data transferred

In providing the service, the parties process Customer Personal Data limited to, for the purposes of this Addendum, pseudonymous identifiers (i.e., IP addresses); and other data relating to a particular device used to navigate the internet, including non-precise location information (derived from IP address intelligence). Customer Personal Data does not contain any names, phone numbers, e-mail addresses, persistent device identifiers or other contact details.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

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

Continuous

Nature of the processing

IAS as Controller: *Ad fraud services*. In addition to identifying invalid traffic which includes specific attempts at ad fraud for individual customers, IAS collects IP Addresses from pixels

embedded in all of its customers' ads, as well as SDKs integrated into ad servers, video players, and mobile applications, and analyses them to identify anomalies that indicate non-human traffic. This information is collected across all IAS channels, customers, and platforms and is aggregated together to create scalable detection models, which allow IAS to distinguish real human behaviour from bot behaviour.

IAS as Processor: Non-precise *Geo-verification*. IAS customers can verify the non-precise location of viewers of a particular webpage or mobile application to ensure they do not serve ads irrelevant to, or inappropriate for, a particular jurisdiction. To do this, IAS obtains information from a device or browser to allow it to detect the approximate (but not precise) location of that IP address. IAS only uses this information to provide non-precise geo- verification services to the specific customer that has requested it, and not for any other purpose, acting only on a specific customer's instructions.

Purpose(s) of the data transfer and further processing

To provide the Services outlined in the Underlying Agreement.

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

IAS retains IP addresses for no longer than thirty (30) days.

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

A current list of sub-processors can be found at Annex 3 and IAS List of Sub-processors.

C. Competent Supervisory Authority

The Supervisory Authority identified in the Underlying Agreement.

Annex II to Schedule 2

Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

IAS technical and organizational measures are available at https://go.integralads.com/rs/469-VBI-606/images/IAS-Technical-and-Organizational-Security-Measures.pdf

Annex III to Schedule 2

List of Sub-Processors

Where IAS acts as a Processor, IAS's Sub-Processors can be found here https://integralads.com/ias-data-protection-portal/ias-list-of-sub-processors/.

Annex IV to Schedule 2

Supplemental Clauses

1. Supplemental Clauses for Compliance with Swiss Data Protection Law

a. The term "Member State" as used in the European Union's Standard Contractual Clauses for the transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 ("**Standard Contractual Clauses**"), including these Annexes, shall be interpreted as including Switzerland.

b. The term "Data Subjects" as used in the Standard Contractual Clauses, including these Annexes shall be interpreted as including Data Subjects in Switzerland.

c. Data subjects with their regular place of residence in Switzerland may bring a lawsuit in Switzerland against either the data exporter or the data importer in accordance with Clause 18(c) of the Standard Contractual Clauses.

d. The Standard Contractual Clauses will additionally protect data pertaining to Swiss legal entities until the revised Swiss Federal Act on Data Protection enters into force.

e. Switzerland's Federal Data Protection and Information Commissioner shall be the competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses with respect to the Personal Data of Swiss residents.

2. Standard Data Protection Clauses to be issued by the Information Commissioner under S119A(1) Data Protection Act 2018 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses – VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the UK Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Same as the date of last signature provided in Annex I above.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Annex I above.	See Annex I above.
Key Contact	See Annex I above.	See Annex I above.

Table 2: Selected SCCs, Modules and Selected Clauses

<table>
<tr><td colspan="2"><b>Addendum EU SCCs</b></td><td colspan="5">☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:</td></tr>
<tr><td>Module</td><td>Module in operation</td><td>Clause 7 (Docking Clause)</td><td>Clause 11 (Option)</td><td>Clause 9a (Prior Authorisation or General Authorisation)</td><td>Clause 9a (Time period)</td><td>Is personal data received from the Importer combined with personal data collected by the Exporter?</td></tr>
<tr><td>1</td><td>In effect</td><td>Not in effect</td><td>Not in effect</td><td></td><td></td><td></td></tr>
</table>

2	In effect	Not in effect	Not in effect	Option II Prior General Authorisation	15 calendar days	
3	N/A	N/A	N/A	N/A		
4	N/A	N/A	N/A			N/A

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: **See Annex I.A**

Annex 1B: Description of Transfer: **See Annex I.B**

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

Annex III: List of Sub processors (Modules 2 and 3 only): **Not applicable**

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	☐ Importer ☐ Exporter ☒ Neither Party

Part 2: Mandatory Clauses **Mandatory Clauses**	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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** of those Mandatory Clauses.

Schedule 3

AUSTRALIAN PRIVACY ACT SUPPLEMENT

This Australian Privacy Act data protection supplement (the "**Privacy Act Supplement**") provides additional responsibilities of the Parties with respect to the processing of Customer Personal Data to the Privacy Act 1988 and processed in the course of Customer's use of the Services.

In the event of any conflict or inconsistency between the MSA, SOW and this Privacy Act Annex, this Privacy Act Annex shall govern.

1. Additional Obligations on IAS.

   a. IAS shall not, directly or indirectly, use or disclose the Personal Data unless necessary to provide the Services.

   b. IAS shall not send Customer Personal Data to any location outside of Australia or the United States of America, including for storage, unless authorization is received from Customer in writing.

Schedule 4

SINGAPORE PERSONAL DATA PROTECTION ACT 2012 (“PDPA”) SUPPLEMENT

This Singapore Personal Data Protection Act 2012 Supplement (the **“PDPA Supplement”**) provides additional responsibilities of the Parties with respect to the processing of Customer Personal Data subject to the Personal Data Protection Act 2012 (“**PDPA**”) processed in the course of Customer’s use of the Services.

1. In the course of providing the Services to Customer, IAS may collect and/or use IP addresses from viewers of Customer’s advertisements in order to conduct invalid traffic analysis (which includes ad fraud analysis). IP addresses may be considered “**PDPA Personal Data**” (defined below in 1.a) under the PDPA if combined with other information IAS has (or is likely to have access to) such that an individual becomes identifiable.

   a. “**PDPA Personal Data**” means data, whether true or not, about an individual who can be identified (i) from that data; or (ii) from that data in combination with other information to which IAS has or is likely to have access.

   b. Because an individual cannot be identified solely from the data collected by IAS or from that data in combination with other information collected or maintained by IAS, the Parties hereby agree that the Customer Personal Data processed in providing the Services to Customer is not PDPA Personal Data, and the PDPA is not applicable.

   c. In the event that IAS’s collection and/or use of Customer Personal Data changes, such that it is considered PDPA Personal Data subject to compliance with the PDPA, the Parties agree to amend this PDPA Supplement as necessary to ensure that the provision of the Services complies with the PDPA’s requirements, including any transfer obligations.